

J.W. Price  
949/261.8433  
makoto Tatebayashi et al.

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT  
NAK1-BI69

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application:

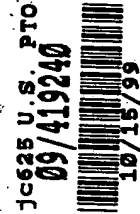
1998年10月16日

出 願 番 号  
Application Number:

平成10年特許願第295920号

出 願 人  
Applicant(s):

松下電器産業株式会社

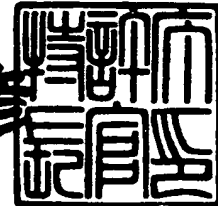


CERTIFIED COPY OF  
PRIORITY DOCUMENT

1999年10月 1日

特許庁長官  
Commissioner,  
Patent Office

近藤 隆彦



【書類名】 特許願

【整理番号】 2022500408

【提出日】 平成10年10月16日

【あて先】 特許庁長官 殿

【国際特許分類】 G09C 1/00

【発明の名称】 デジタル著作物保護システム

【請求項の数】 17

【発明者】

【住所又は居所】 大阪府門真市大字門真 1006番地 松下電器産業株式会社内

【氏名】 館林 誠

【発明者】

【住所又は居所】 大阪府門真市大字門真 1006番地 松下電器産業株式会社内

【氏名】 中村 穰

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100090446

【弁理士】

【氏名又は名称】 中島 司朗

【代理人】

【識別番号】 100109210

【弁理士】

【氏名又は名称】 新居 広守

【手数料の表示】

【予納台帳番号】 014823

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9810105

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 デジタル著作物保護システム

【特許請求の範囲】

【請求項 1】 記録媒体とアクセス装置とが接続された状態で、両者間で機器認証フェーズと著作物転送フェーズとを実行して著作物の正当者への配布を実現するデジタル著作物保護システムであって、

機器認証フェーズでは、記録媒体が所有する固有鍵をアクセス装置に秘密伝送し、アクセス装置が取得した固有鍵を用いて、機器認証を行い、

著作物転送フェーズでは、機器認証が成功した場合にのみ、アクセス装置が取得した固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する

ことを特徴とするデジタル著作物保護システム。

【請求項 2】 記録媒体とアクセス装置とが接続された状態で、前記記録媒体と前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行うデジタル著作物保護システムであって、

前記記録媒体は、

記録媒体毎に異なる固有鍵を予め記憶している固有鍵記憶領域と、

接続されたアクセス装置へ前記固有鍵を秘密伝送し、前記固有鍵を用いて前記アクセス装置との間で機器認証を行う第 1 認証手段と、

前記固有鍵を用いて暗号化される著作物を保持するための領域とを備え、

前記アクセス装置は、

記録媒体から秘密伝送された固有鍵を用いて、前記記録媒体との間で機器認証を行う第 2 認証手段と、

機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送手段とを備える

ことを特徴とするデジタル著作物保護システム。

【請求項 3】 前記第 1 認証手段は、あらかじめ第 1 鍵を有し、前記第 1 鍵を用いて、前記固有鍵に第 1 暗号を施して暗号化固有鍵を生成して伝送し、

前記第 2 認証手段は、あらかじめ前記第 1 鍵を有し、前記第 1 鍵を用いて、前記伝送された暗号化固有鍵に、前記第 1 暗号の逆変換を行う第 1 復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送手段は、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項 2 記載のデジタル著作物保護システム。

【請求項 4】 前記第 1 認証手段は、第 1 鍵を基にして、公開鍵暗号方式の公開鍵決定アルゴリズムにより算出された公開鍵である第 2 鍵をあらかじめ有し、前記第 2 鍵を用いて、前記固有鍵に第 1 暗号を施して暗号化固有鍵を生成して伝送し、

前記第 2 認証手段は、あらかじめ前記第 1 鍵を有し、前記第 1 鍵を用いて、前記伝送された暗号化固有鍵に、前記第 1 暗号の逆変換を行う第 1 復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送手段は、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項 2 記載のデジタル著作物保護システム。

【請求項 5】 前記第 1 認証手段は、あらかじめ第 1 鍵を有し、前記第 1 鍵を用いて、前記固有鍵に回復型署名処理を施して署名文を生成して伝送し、

前記第 2 認証手段は、前記第 1 鍵に前記回復型署名処理の公開鍵決定アルゴリズムにより算出された公開鍵である第 2 鍵をあらかじめ有し、前記第 2 鍵を用いて、前記伝送された署名文に、前記回復型署名の検証処理を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送手段は、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項 2 記載のデジタル著作物保護システム。

【請求項 6】 前記デジタル著作物保護システムは、さらに

固有鍵に第 1 暗号を施して暗号化固有鍵に変換する固有鍵変換手段を備える暗号化固有鍵作成装置を有し、

前記第 1 認証手段は、前記固有鍵を前記固有鍵変換手段へ出力して暗号化固有鍵に変換し、変換された暗号化固有鍵を前記アクセス装置へ伝送し、

前記第 2 認証手段は、記録媒体から伝送された暗号化固有鍵に前記第 1 暗号の逆処理を行う第 1 復号を施して固有鍵を生成する

ことを特徴とする請求項 2 記載のデジタル著作物保護システム。

【請求項 7】 前記第 1 認証手段は、あらかじめ複数の第 1 鍵を有し、前記複数の第 1 鍵のうち一つの第 2 鍵の選択を受け付け、前記第 2 鍵を用いて、前記固有鍵に第 1 暗号を施して暗号化固有鍵を生成して伝送し、

前記第 2 認証手段は、あらかじめ複数の第 1 鍵を有し、前記複数の第 1 鍵から前記第 2 鍵の選択を受け付け、前記第 2 鍵を用いて、前記伝送された暗号化固有鍵に、前記第 1 暗号の逆変換を行う第 1 復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送手段は、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項 2 記載のデジタル著作物保護システム。

【請求項 8】 アクセス装置と接続された状態で、前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行う記録媒体であって、

記録媒体毎に異なる固有鍵を記憶している固有鍵記憶領域と、

前記固有鍵を用いて暗号化される著作物を保持するための領域と、

アクセス装置が接続されたとき、記録媒体から当該アクセス装置へ固有鍵を秘密伝送する手順を経て、当該アクセス装置との間で機器認証を行う認証手段と、

機器認証が成功した場合にのみ、前記固有鍵を用いて暗号化された著作物を受け取り前記領域に書き込み若しくは前記領域に記憶されている暗号化された著作物を読み出して前記アクセス装置へ出力する転送手段と

を備えることを特徴とする記録媒体。

【請求項 9】 固有鍵を有する記録媒体と接続され、前記記録媒体との間で機器認証と暗号化された著作物の転送とを行うアクセス装置であって、

記録媒体から固有鍵を秘密伝送される手順を経て、前記記録媒体との間で機器認証を行う認証手段と、

機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送手段と

を備えることを特徴とするアクセス装置。

【請求項 10】 記録媒体とアクセス装置とが接続された状態で、両者間で機器認証ステップと著作物転送ステップとを実行して著作物の正当者への配布を実現するデジタル著作物保護方法であって、

機器認証ステップでは、記録媒体が所有する固有鍵をアクセス装置に秘密伝送し、アクセス装置が取得した固有鍵を用いて、機器認証を行い、

著作物転送ステップでは、機器認証が成功した場合にのみ、アクセス装置が取得した固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する

ことを特徴とするデジタル著作物保護方法。

【請求項 11】 記録媒体毎に異なる固有鍵を予め記憶している固有鍵記憶領域及び前記固有鍵を用いて暗号化される著作物を保持するための領域を有する記録媒体とアクセス装置とが接続された状態で、前記記録媒体と前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行うデジタル著作物保護システムで用いられるデジタル著作物保護方法であって、

接続されたアクセス装置へ前記固有鍵を秘密伝送し、前記固有鍵を用いて前記アクセス装置との間で機器認証を行う第 1 認証ステップと、

記録媒体から秘密伝送された固有鍵を用いて、前記記録媒体との間で機器認証を行う第 2 認証ステップと、

機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送ステップとを

含むことを特徴とするデジタル著作物保護方法。

【請求項 12】 前記第 1 認証ステップは、あらかじめ第 1 鍵を有し、前記第 1 鍵を用いて、前記固有鍵に第 1 暗号を施して暗号化固有鍵を生成して伝送し、

前記第 2 認証ステップは、あらかじめ前記第 1 鍵を有し、前記第 1 鍵を用いて、前記伝送された暗号化固有鍵に、前記第 1 暗号の逆変換を行う第 1 復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行う  
ことを特徴とする請求項 11 記載のデジタル著作物保護方法。

【請求項 13】 前記第 1 認証ステップは、第 1 鍵を基にして、公開鍵暗号方式の公開鍵決定アルゴリズムにより算出された公開鍵である第 2 鍵をあらかじめ有し、前記第 2 鍵を用いて、前記固有鍵に第 1 暗号を施して暗号化固有鍵を生成して伝送し、

前記第 2 認証ステップは、あらかじめ前記第 1 鍵を有し、前記第 1 鍵を用いて、前記伝送された暗号化固有鍵に、前記第 1 暗号の逆変換を行う第 1 復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行う  
ことを特徴とする請求項 11 記載のデジタル著作物保護方法。

【請求項 14】 前記第 1 認証ステップは、あらかじめ第 1 鍵を有し、前記第 1 鍵を用いて、前記固有鍵に回復型署名処理を施して署名文を生成して伝送し、

前記第 2 認証ステップは、前記第 1 鍵に前記回復型署名処理の公開鍵決定アルゴリズムにより算出された公開鍵である第 2 鍵をあらかじめ有し、前記第 2 鍵を用いて、前記伝送された署名文に、前記回復型署名の検証処理を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行う  
ことを特徴とする請求項 11 記載のデジタル著作物保護方法。

【請求項 15】 前記デジタル著作物保護システムは、さらに固有鍵に第 1 暗号を施して暗号化固有鍵に変換する固有鍵変換手段を備える暗号化固有鍵作成装置を有し、

前記第 1 認証ステップは、前記固有鍵を前記固有鍵変換手段へ出力して暗号化固有鍵に変換し、変換された暗号化固有鍵を前記アクセス装置へ伝送し、

前記第 2 認証ステップは、記録媒体から伝送された暗号化固有鍵に前記第 1 暗号の逆処理を行う第 1 復号を施して固有鍵を生成する

ことを特徴とする請求項 11 記載のデジタル著作物保護方法。

【請求項 16】 前記第 1 認証ステップは、あらかじめ複数の第 1 鍵を有し、



前記複数の第1鍵のうち一つの第2鍵の選択を受け付け、前記第2鍵を用いて、前記固有鍵に第1暗号を施して暗号化固有鍵を生成して伝送し、

前記第2認証ステップは、あらかじめ複数の第1鍵を有し、前記複数の第1鍵から前記第2鍵の選択を受け付け、前記第2鍵を用いて、前記伝送された暗号化固有鍵に、前記第1暗号の逆変換を行う第1復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項11記載のデジタル著作物保護方法。

【請求項17】 デジタル著作物保護方法をコンピュータに実行させるためのプログラムを記録するコンピュータ読み取り可能な媒体であって、

請求項10～16記載の何れかのデジタル著作物保護方法をコンピュータに実行させるためのプログラムを含むことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタル化された文書、音声、画像、プログラムなどのデジタル著作物をネットワークで配信し、これを記憶媒体に記録し、携帯プレーヤで再生するシステムに関し、特に、不正にこれらの記録や再生が行われることを防ぐシステムに関する。

【0002】

【従来の技術】

近年、デジタル化された文書、音声、画像、プログラムなどのデジタル著作物がインターネットなどのネットワークを経由して流通し、利用者は、様々なデジタル著作物を簡単にネットワークを経由して取り出し、他の記録媒体に記録し、再生することができるようになってきている。

【0003】

【発明が解決しようとする課題】

しかしながら、このように簡単にデジタル著作物を複製できるという利点はあるものの、著作者の著作権が侵害されやすいという問題点がある。

本発明は、外部から取り出したデジタル著作物を不正に記録媒体へ書き込むことと、記録媒体に記録されたデジタル著作物を不正に再生することを防止するデジタル著作物保護システムを提供することを目的とする。

## 【0004】

## 【課題を解決するための手段】

上記の目的を達成するために、本発明は、記録媒体とアクセス装置とが接続された状態で、両者間で機器認証フェーズと著作物転送フェーズとを実行して著作物の正当者への配布を実現するデジタル著作物保護システムであって、機器認証フェーズでは、記録媒体が所有する固有鍵をアクセス装置に秘密伝送し、アクセス装置が取得した固有鍵を用いて、機器認証を行い、著作物転送フェーズでは、機器認証が成功した場合にのみ、アクセス装置が取得した固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号することを特徴とする。

## 【0005】

ここで、記録媒体とアクセス装置とが接続された状態で、前記記録媒体と前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行うデジタル著作物保護システムであって、前記記録媒体は、記録媒体毎に異なる固有鍵を予め記憶している固有鍵記憶領域と、接続されたアクセス装置へ前記固有鍵を秘密伝送し、前記固有鍵を用いて前記アクセス装置との間で機器認証を行う第1認証手段と、前記固有鍵を用いて暗号化される著作物を保持するための領域とを備え、前記アクセス装置は、記録媒体から秘密伝送された固有鍵を用いて、前記記録媒体との間で機器認証を行う第2認証手段と、機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送手段とを備えるように構成してもよい。

## 【0006】

ここで、前記第1認証手段は、あらかじめ第1鍵を有し、前記第1鍵を用いて、前記固有鍵に第1暗号を施して暗号化固有鍵を生成して伝送し、前記第2認証手段は、あらかじめ前記第1鍵を有し、前記第1鍵を用いて、前記伝送された暗

号化固有鍵に、前記第 1 暗号の逆変換を行う第 1 復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

## 【0007】

ここで、前記第 1 認証手段は、第 1 鍵を基にして、公開鍵暗号方式の公開鍵決定アルゴリズムにより算出された公開鍵である第 2 鍵をあらかじめ有し、前記第 2 鍵を用いて、前記固有鍵に第 1 暗号を施して暗号化固有鍵を生成して伝送し、前記第 2 認証手段は、あらかじめ前記第 1 鍵を有し、前記第 1 鍵を用いて、前記伝送された暗号化固有鍵に、前記第 1 暗号の逆変換を行う第 1 復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

## 【0008】

ここで、前記第 1 認証手段は、あらかじめ第 1 鍵を有し、前記第 1 鍵を用いて、前記固有鍵に回復型署名処理を施して署名文を生成して伝送し、前記第 2 認証手段は、前記第 1 鍵に前記回復型署名処理の公開鍵決定アルゴリズムにより算出された公開鍵である第 2 鍵をあらかじめ有し、前記第 2 鍵を用いて、前記伝送された署名文に、前記回復型署名の検証処理を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

## 【0009】

ここで、前記デジタル著作物保護システムは、さらに固有鍵に第 1 暗号を施して暗号化固有鍵に変換する固有鍵変換手段を備える暗号化固有鍵作成装置を有し、前記第 1 認証手段は、前記固有鍵を前記固有鍵変換手段へ出力して暗号化固有鍵に変換し、変換された暗号化固有鍵を前記アクセス装置へ伝送し、前記第 2 認証手段は、記録媒体から伝送された暗号化固有鍵に前記第 1 暗号の逆処理を行う第 1 復号を施して固有鍵を生成するように構成してもよい。

## 【0010】

ここで、前記第 1 認証手段は、あらかじめ複数の第 1 鍵を有し、前記複数の第

1 鍵のうち一つの第 2 鍵の選択を受け付け、前記第 2 鍵を用いて、前記固有鍵に第 1 暗号を施して暗号化固有鍵を生成して伝送し、前記第 2 認証手段は、あらかじめ複数の第 1 鍵を有し、前記複数の第 1 鍵から前記第 2 鍵の選択を受け付け、前記第 2 鍵を用いて、前記伝送された暗号化固有鍵に、前記第 1 暗号の逆変換を行う第 1 復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

#### 【0011】

また、本発明は、アクセス装置と接続された状態で、前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行う記録媒体であって、記録媒体毎に異なる固有鍵を記憶している固有鍵記憶領域と、前記固有鍵を用いて暗号化される著作物を保持するための領域と、アクセス装置が接続されたとき、記録媒体から当該アクセス装置へ固有鍵を秘密伝送する手順を経て、当該アクセス装置との間で機器認証を行う認証手段と、機器認証が成功した場合にのみ、前記固有鍵を用いて暗号化された著作物を受け取り前記領域に書き込み若しくは前記領域に記憶されている暗号化された著作物を読み出して前記アクセス装置へ出力する転送手段とを備えることを特徴とする。

#### 【0012】

また、本発明は、固有鍵を有する記録媒体と接続され、前記記録媒体との間で機器認証と暗号化された著作物の転送とを行うアクセス装置であって、記録媒体から固有鍵を秘密伝送される手順を経て、前記記録媒体との間で機器認証を行う認証手段と、機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送手段とを備えることを特徴とする。

#### 【0013】

#### 【発明の実施の形態】

本発明に係る一つの実施の形態としてのデジタル著作物保護システム 100 について説明する。

## 1. デジタル著作物保護システム 100 の構成

デジタル著作物保護システム 100 は、図 1 のブロック図に示すように、メモ리카ード 200、メモ리카ードライター 300、メモ리카ードリーダー 400 から構成される。

### 【0014】

メモ리카ード 200 は、図 2 に示すように、メモ리카ード挿入口 301 から挿入され、メモ리카ードライター 300 に装着される。また、メモ리카ードライター 300 は、メモ리카ードライター挿入口 501 から挿入され、パーソナルコンピュータ 500 に装着される。メモ리카ードライター 300 は、パーソナルコンピュータ 500 を介在して通信回線 10 により外部と接続されている。

### 【0015】

パーソナルコンピュータ 500 は、ディスプレイ 503、キーボード 504、スピーカ 502、図示していないプロセッサ、RAM、ROM、ハードディスク装置を備えている。

メモ리카ード 200 は、メモ리카ードリーダー 400 に装着される。メモ리카ード 200 は、図 3 に示すように、メモ리카ード挿入口 403 から挿入されて、メモ리카ードリーダー 400 の一つの実施例としてのヘッドホンステレオ 401 に装着される。ヘッドホンステレオ 401 は、上面に操作ボタン 404 a、404 b、404 c、404 d が配置され、側面にメモ리카ード挿入口 403 を有し、別の側面にヘッドホン 402 が接続されている。

## 1. 1 メモ리카ード 200 の構成

メモ리카ード 200 は、図 4 に示すように、マスタ鍵記憶部 210、メディア固有鍵記憶部 220、変換部 230、メディア固有鍵情報記憶部 240、装置鍵記憶部 221、逆変換部 222、装置鍵情報記憶部 223、相互認証部 250、暗号化著作物記憶部 260、通信部 270、制御部 280 から構成される。

### 【0016】

メモ리카ード 200 がメモ리카ードライター 300 に装着されると、通信部 270 は、メモ리카ードライター 300 の後述する通信部 340 と接続される。

メモ리카ード200がメモ리카ードリーダ400に装着されると、通信部270は、メモ리카ードリーダ400の後述する通信部440と接続される。

#### 1. 1. 1 マスタ鍵記憶部210

マスタ鍵記憶部210は、あらかじめ一つのマスタ鍵Mkを記憶している。マスタ鍵Mkは、56ビットのビット列からなる。マスタ鍵は、デジタル著作物運用システム毎に異なる。さらに、特定のデジタル著作物運用システム用メモ리카ードを製造するすべてのメーカーにより製造されたすべてのメモ리카ードのマスタ鍵記憶部には、同じマスタ鍵が記憶されている。

【0017】

ここで、デジタル著作物運用システムとは、例えば、A社、B社、C社の3者が共同で運営し、音楽を配信する音楽配信システムであり、また、X社、Y社、Z社が共同で運営する映画レンタルシステムである。

#### 1. 1. 2 メディア固有鍵記憶部220

メディア固有鍵記憶部220は、あらかじめ一つの固有鍵Kiを記憶している。固有鍵Kiは、56ビットのビット列からなる。固有鍵は、メモ리카ード毎に異なる。固有鍵は、メモ리카ード毎に異なるメモ리카ードの製造番号と、その都度生成される乱数とに、所定の演算を施して、例えば加算を施して算出される。

#### 1. 1. 3 変換部230

変換部230は、メディア固有鍵記憶部220に記憶されている固有鍵Kiを読み出し、マスタ鍵記憶部210に記憶されているマスタ鍵Mkを読み出す。

【0018】

変換部230は、DES（データ暗号化規格、Data Encryption Standard）により規格されている暗号アルゴリズムE1をあらかじめ記憶している。

ここで、DESにより規格されている暗号アルゴリズムE1は、暗号鍵は56ビットであり、平文及び暗号文の長さは64ビットである。なお、この実施の形

態において、暗号アルゴリズム及び復号アルゴリズムは、特に断らない限り、DESにより規格されているアルゴリズムであり、暗号鍵及び復号鍵は56ビットであり、平文及び暗号文の長さは64ビットである。

【0019】

変換部230は、読み出した固有鍵 $K_i$ に暗号アルゴリズム $E_1$ を施して暗号化固有鍵 $J_i$ を生成する。このとき、前記読み出したマスタ鍵 $M_k$ を暗号アルゴリズム $E_1$ の鍵とする。生成された暗号化固有鍵 $J_i$ は式1に示すように表現できる。

$$(式1) \quad J_i = E_1 (M_k, K_i)$$

なお、この明細書において、鍵 $K$ を用いて、平文 $M$ に対して、暗号アルゴリズム $E$ を施し、暗号文 $C$ を生成するとき、式2に示すように表現することとする。

$$(式2) \quad C = E (K, M)$$

また、鍵 $K$ を用いて、前記生成された暗号文 $C$ に対して、復号アルゴリズム $D$ を施して、前記平文 $M$ を生成するとき、式3に示すように表現することとする。

$$(式3) \quad M = D (K, C)$$

このように、鍵 $K$ を用いて、平文 $M$ に対して、暗号アルゴリズム $E$ を施し暗号文 $C$ を生成し、生成された暗号文 $C$ に対して、復号アルゴリズム $D$ を施して、前記平文 $M$ と同一の平文が生成されるとき、暗号アルゴリズム $E$ と復号アルゴリズム $D$ との関係を式4に示すように表現することとする。

$$(式4) \quad E = D^{-1}$$

変換部230は、生成した暗号化固有鍵 $J_i$ をメディア固有鍵情報記憶部240へ出力する。

#### 1. 1. 4 メディア固有鍵情報記憶部240

メディア固有鍵情報記憶部240は、変換部230から、暗号化固有鍵 $J_i$ を受け取り、受け取った暗号化固有鍵 $J_i$ を記憶する。

#### 1. 1. 5 相互認証部250

相互認証部250は、乱数発生部251、暗号部252、復号部253、相互

認証制御部 254 から構成される。

(1) 乱数発生部 251

乱数発生部 251 は、乱数 R2 を生成する。乱数 R2 は、64 ビットのビット列からなる。乱数発生部 251 は、生成した乱数 R2 を通信部 270 と相互認証制御部 254 とへ出力する。

(2) 暗号部 252

暗号部 252 は、通信部 270 から乱数 R1 を受け取る。

【0020】

暗号部 252 は、メディア固有鍵記憶部 220 から固有鍵 K<sub>i</sub> を読み出す。

暗号部 252 は、DES により規格されている暗号アルゴリズム E2 をあらかじめ記憶している。

暗号部 252 は、受け取った乱数 R1 に暗号アルゴリズム E2 を施して暗号化乱数 S1 を生成する。このとき、前記読み出した固有鍵 K<sub>i</sub> を暗号アルゴリズム E2 の鍵とする。生成された暗号化乱数 S1 は式 5 に示すように表現できる。

$$(式5) \quad S1 = E2 (K_i, R1)$$

暗号部 252 は、生成した暗号化乱数 S1 を通信部 270 へ出力する。

(3) 復号部 253

復号部 253 は、通信部 270 から暗号化乱数 S2 を受け取り、装置鍵記憶部 221 から装置鍵 A' <sub>j</sub> を読み出す。

【0021】

復号部 253 は、DES により規格されている復号アルゴリズム D2 をあらかじめ記憶している。

復号部 253 は、受け取った暗号化乱数 S2 に復号アルゴリズム D2 を施して乱数 R' <sub>2</sub> を生成する。このとき、前記読み出した装置鍵 A' <sub>j</sub> を復号アルゴリズム D2 の鍵とする。生成された乱数 R' <sub>2</sub> は式 6 に示すように表現できる。

$$(式6) \quad R' 2 = D2 (A' j, S2)$$



$$=D2(A'j, E2(Aj, R2))$$

復号部 253 は、生成した乱数  $R'2$  を相互認証制御部 254 へ出力する。

#### (4) 相互認証制御部 254

相互認証制御部 254 は、復号部 253 から乱数  $R'2$  を受け取る。また、相互認証制御部 254 は、乱数発生部 251 から乱数  $R2$  を受け取る。

##### 【0022】

相互認証制御部 254 は、復号部 253 から受け取った乱数  $R'2$  と、乱数発生部 251 から受け取った乱数  $R2$  とを比較し、乱数  $R'2$  と乱数  $R2$  とが一致すれば、メモリカード 200 が装着されたメモリカードライタ 300 又はメモリカードリーダー 400 が正しい装置であると認証し、乱数  $R'2$  と乱数  $R2$  とが一致していなければ、メモリカード 200 が装着されたメモリカードライタ 300 又はメモリカードリーダー 400 が不正な装置であるとみなす。

##### 【0023】

相互認証制御部 254 は、メモリカードライタ 300 又はメモリカードリーダー 400 が正しい装置であるか、不正な装置であるかを示す認証信号を制御部 280 へ出力する。

#### 1. 1. 6 暗号化著作物記憶部 260

暗号化著作物記憶部 260 は、記憶媒体として半導体メモリを有する。

##### 【0024】

暗号化著作物記憶部 260 は、通信部 270 から暗号化部分著作物  $Fi$  ( $i = 1, 2, 3, \dots$ ) を受け取り、受け取った暗号化部分著作物  $Fi$  ( $i = 1, 2, 3, \dots$ ) を記憶する。

#### 1. 1. 7 通信部 270

通信部 270 は、メディア固有鍵情報記憶部 240 から暗号化固有鍵  $Ji$  を読み出し、読み出した暗号化固有鍵  $Ji$  をメモリカードライタ 300 の通信部 340 又はメモリカードリーダー 400 の通信部 440 へ出力する。

【0025】

通信部 270 は、メモリカードライタ 300 の通信部 340 から又はメモリカードリーダ 400 の通信部 440 から乱数 R1 を受け取り、受け取った乱数 R1 を相互認証部 250 の暗号部 252 へ出力する。

通信部 270 は、暗号部 252 から暗号化乱数 S1 を受け取り、受け取った暗号化乱数 S1 をメモリカードライタ 300 の通信部 340 又はメモリカードリーダ 400 の通信部 440 へ出力する。

【0026】

通信部 270 は、メモリカードライタ 300 の通信部 340 又はメモリカードリーダ 400 の通信部 440 から、暗号化装置鍵 Bj を受け取り、受け取った暗号化装置鍵 Bj を装置鍵情報記憶部 223 へ出力する。

通信部 270 は、乱数発生部 251 から乱数 R2 を受け取り、受け取った乱数 R2 をメモリカードライタ 300 の通信部 340 又はメモリカードリーダ 400 の通信部 440 へ出力する。

【0027】

通信部 270 は、メモリカードライタ 300 の通信部 340 又はメモリカードリーダ 400 の通信部 440 から暗号化乱数 S2 を受け取り、受け取った暗号化乱数 S2 を相互認証部 250 の復号部 253 へ出力する。

通信部 270 は、制御部 280 から通信中止信号を受け取ると、メモリカードライタ 300 の通信部 340 又はメモリカードリーダ 400 の通信部 440 との通信を中止する。

【0028】

通信部 270 は、メモリカードライタ 300 の通信部 340 から暗号化部分著作物 Fi ( $i = 1, 2, 3, \dots$ ) を受け取り、受け取った暗号化部分著作物 Fi ( $i = 1, 2, 3, \dots$ ) を暗号化著作物記憶部 260 へ出力する。

通信部 270 は、暗号化著作物記憶部 260 から暗号化著作物を読み出し、読み出した暗号化著作物をメモリカードリーダ 400 の通信部 440 へ出力する。

1. 1. 8 装置鍵情報記憶部 223

装置鍵情報記憶部 223 は、通信部 270 から暗号化装置鍵 Bj を受け取り、

受け取った暗号化装置鍵  $B_j$  を記憶する。

#### 1. 1. 9 逆変換部 222

逆変換部 222 は、装置鍵情報記憶部 223 から暗号化装置鍵  $B_j$  を読み出し、マスタ鍵記憶部 210 に記憶されているマスタ鍵  $M_k$  を読み出す。

【0029】

逆変換部 222 は、DES により規格されている復号アルゴリズム  $D3$  をあらかじめ記憶している。

逆変換部 222 は、読み出した暗号化装置鍵  $B_j$  に復号アルゴリズム  $D3$  を施して装置鍵  $A'_j$  を生成する。このとき、前記読み出したマスタ鍵  $M_k$  を復号アルゴリズム  $D3$  の鍵とする。生成された装置鍵  $A'_j$  は式 7 に示すように表現できる。

$$\begin{aligned} \text{(式 7)} \quad A'_j &= D3 (M_k, B_j) \\ &= D3 (M_k, E3 (M_k, A_j)) \end{aligned}$$

逆変換部 222 は、生成した装置鍵  $A'_j$  を装置鍵記憶部 221 へ出力する。

#### 1. 1. 10 装置鍵記憶部 221

装置鍵記憶部 221 は、逆変換部 222 から出力された装置鍵  $A'_j$  を記憶する。

#### 1. 1. 11 制御部 280

制御部 280 は、相互認証制御部 254 からメモ리카ード 200 が装着されたメモ리카ードライター 300 又はメモ리카ードリーダー 400 が正しい装置であるか、不正な装置であるかを示す認証信号を受け取る。

【0030】

制御部 280 は、受け取った認証信号が不正な装置であることを示す場合には、メモ리카ードライター 300 又はメモ리카ードリーダー 400 との通信を中止する通信中止信号を通信部 270 へ出力する。

#### 1. 2 メモ리카ードライター 300 の構成

メモリカードライタ 300 は、図 5 に示すように、装置鍵記憶部 310、変換部 311、装置鍵情報記憶部 312、マスタ鍵記憶部 313、メディア固有鍵情報記憶部 320、逆変換部 321、メディア固有鍵記憶部 323、相互認証部 330、通信部 340、制御部 350、暗号部 360、著作物記憶部 370、著作物取得部 380 から構成される。

#### 【0031】

著作物取得部 380 は、通信回線 10 を経由して外部と接続されている。

#### 1. 2. 1 装置鍵記憶部 310

装置鍵記憶部 310 は、あらかじめ一つの装置鍵  $A_j$  を記憶している。装置鍵  $A_j$  は、56 ビットのビット列からなる。装置鍵は、メモリカードライタ毎に異なる。装置鍵は、メモリカードライタ毎に異なるメモリカードライタの製造番号と、その都度生成される乱数とに、所定の演算を施して、例えば加算を施して算出される。

#### 1. 2. 2 変換部 311

変換部 311 は、装置鍵記憶部 310 に記憶されている装置鍵  $A_j$  を読み出し、マスタ鍵記憶部 313 に記憶されているマスタ鍵  $M_k$  を読み出す。

#### 【0032】

変換部 311 は、DES により規格されている暗号アルゴリズム  $E_3$  をあらかじめ記憶している。

メモリカード 200 の逆変換部 222 に記憶されている復号アルゴリズム  $D_3$  と暗号アルゴリズム  $E_3$  との間には、式 8 に示す関係がある。

$$(式 8) \quad E_3 = D_3^{-1}$$

変換部 311 は、読み出した装置鍵  $A_j$  に暗号アルゴリズム  $E_3$  を施して暗号化装置鍵  $B_j$  を生成する。このとき、前記読み出したマスタ鍵  $M_k$  を暗号アルゴリズム  $E_3$  の鍵とする。生成された暗号化装置鍵  $B_j$  は式 9 に示すように表現できる。

$$(式 9) \quad B_j = E_3 (M_k, A_j)$$

変換部 311 は、生成した暗号化装置鍵  $B_j$  を装置鍵情報記憶部 312 へ出力する。

#### 1. 2. 3 装置鍵情報記憶部 312

装置鍵情報記憶部 312 は、変換部 311 から暗号化装置鍵  $B_j$  を受け取り、受け取った暗号化装置鍵  $B_j$  を記憶する。

#### 1. 2. 4 マスタ鍵記憶部 313

マスタ鍵記憶部 313 は、あらかじめ一つのマスタ鍵  $M_k$  を記憶している。マスタ鍵  $M_k$  は、メモリカード 200 のマスタ鍵記憶部 210 が記憶しているマスタ鍵と同じである。

#### 1. 2. 5 メディア固有鍵情報記憶部 320

メディア固有鍵情報記憶部 320 は、通信部 340 から暗号化固有鍵  $J_i$  を受け取り、受け取った暗号化固有鍵  $J_i$  を記憶する。

#### 1. 2. 6 逆変換部 321

逆変換部 321 は、メディア固有鍵情報記憶部 320 に記憶されている暗号化固有鍵  $J_i$  を読み出し、マスタ鍵記憶部 313 に記憶されているマスタ鍵  $M_k$  を読み出す。

【0033】

逆変換部 321 は、DES により規格されている復号アルゴリズム  $D1$  をあらかじめ記憶している。

メモリカード 200 の変換部 230 に記憶されている暗号アルゴリズム  $E1$  と復号アルゴリズム  $D1$  との間には、式 10 に示す関係がある。

$$(式 10) \quad E1 = D1^{-1}$$

逆変換部 321 は、読み出した暗号化固有鍵  $J_i$  に復号アルゴリズム  $D1$  を施して固有鍵  $K'_i$  を生成する。このとき、前記読み出したマスタ鍵  $M_k$  を復号アルゴリズム  $D1$  の鍵とする。生成された固有鍵  $K'_i$  は、式 11 に示すように表

現できる。

$$\begin{aligned} \text{(式 1 1)} \quad K' i &= D1 (Mk, Ji) \\ &= D1 (Mk, E1 (Mk, Ki)) \end{aligned}$$

逆変換部 3 2 1 は、生成した固有鍵  $K' i$  をメディア固有鍵記憶部 3 2 3 へ出力する。

#### 1. 2. 7 メディア固有鍵記憶部 3 2 3

メディア固有鍵記憶部 3 2 3 は、逆変換部 3 2 1 から固有鍵  $K' i$  を受け取り、受け取った固有鍵  $K' i$  を記憶する。

#### 1. 2. 8 相互認証部 3 3 0

相互認証部 3 3 0 は、乱数発生部 3 3 1、暗号部 3 3 2、復号部 3 3 3、相互認証制御部 3 3 4 から構成される。

##### (1) 乱数発生部 3 3 1

乱数発生部 3 3 1 は、乱数  $R1$  を生成する。乱数  $R1$  は、64 ビットのビット列からなる。乱数発生部 3 3 1 は、生成した乱数  $R1$  を通信部 3 4 0 へ出力する。また、乱数発生部 3 3 1 は、生成した乱数  $R1$  を相互認証制御部 3 3 4 へ出力する。

##### (2) 暗号部 3 3 2

暗号部 3 3 2 は、通信部 3 4 0 から乱数  $R2$  を受け取り、装置鍵記憶部 3 1 0 から装置鍵  $Aj$  を読み出す。

【0034】

暗号部 3 3 2 は、DES により規格されている暗号アルゴリズム  $E2$  をあらかじめ記憶している。

暗号部 3 3 2 は、受け取った乱数  $R2$  に暗号アルゴリズム  $E2$  を施して暗号化乱数  $S2$  を生成する。このとき、前記読み出した装置鍵  $Aj$  を暗号アルゴリズム  $E2$  の鍵とする。生成された暗号化乱数  $S2$  は式 1 2 に示すように表現できる。

(式 12)  $S2 = E2 (Aj, R2)$

暗号部 332 は、生成した暗号化乱数 S2 を通信部 340 へ出力する。

(3) 復号部 333

復号部 333 は、通信部 340 から暗号化乱数 S1 を受け取る。

【0035】

復号部 333 は、メディア固有鍵記憶部 323 から固有鍵  $K'i$  を読み出す。

復号部 333 は、DES により規格されている復号アルゴリズム D2 をあらかじめ記憶している。

メモリカード 200 の相互認証部 330 の暗号部 252 に記憶されている暗号アルゴリズム E2 と復号アルゴリズム D2 との間には、式 13 に示す関係がある。

(式 13)  $E2 = D2^{-1}$

復号部 333 は、受け取った暗号化乱数 S1 に復号アルゴリズム D2 を施して乱数  $R'1$  を生成する。このとき、前記読み出した固有鍵  $K'i$  を復号アルゴリズム D2 の鍵とする。生成された乱数  $R'1$  は式 14 に示すように表現できる。

(式 14)  $R'1 = D2 (K'i, S1)$   
 $= D2 (K'i, E2 (Ki, R1))$

復号部 333 は、生成された乱数  $R'1$  を相互認証制御部 334 へ出力する。

(4) 相互認証制御部 334

相互認証制御部 334 は、復号部 333 から乱数  $R'1$  を受け取る。また、相互認証制御部 334 は、乱数発生部 331 から乱数 R1 を受け取る。

【0036】

相互認証制御部 334 は、復号部 333 から受け取った乱数  $R'1$  と、乱数発生部 331 から受け取った乱数 R1 とを比較し、乱数  $R'1$  と乱数 R1 とが一致すれば、メモリカードライタ 300 に装着されたメモリカード 200 が正しい装置であると認証し、乱数  $R'1$  と乱数 R1 とが一致していなければ、メモリカードライタ 300 に装着されたメモリカード 200 が不正な装置であるとみなす。

【0037】

相互認証制御部 334 は、メモリカードライタ 300 に装着されたメモリカード 200 が正しい装置であるか、不正な装置であるかを示す認証信号を制御部 350 へ出力する。

#### 1. 2. 9 通信部 340

通信部 340 は、メモリカード 200 の通信部 270 から暗号化固有鍵  $J_i$  を受け取り、受け取った暗号化固有鍵  $J_i$  をメディア固有鍵情報記憶部 320 へ出力する。

##### 【0038】

通信部 340 は、乱数発生部 331 から乱数  $R_1$  を受け取り、受け取った乱数  $R_1$  を、メモリカード 200 の通信部 270 へ出力する。

通信部 340 は、メモリカード 200 の通信部 270 から暗号化乱数  $S_1$  を受け取り、受け取った暗号化乱数  $S_1$  を相互認証部 330 の復号部 333 へ出力する。

##### 【0039】

通信部 340 は、装置鍵情報記憶部 312 から暗号化装置鍵  $B_j$  を読み出し、読み出した暗号化装置鍵  $B_j$  をメモリカード 200 の通信部 270 へ出力する。

通信部 340 は、メモリカード 200 の通信部 270 から乱数  $R_2$  を受け取り、受け取った乱数  $R_2$  を相互認証部 330 の暗号部 332 へ出力する。

通信部 340 は、暗号部 332 から暗号化乱数  $S_2$  を受け取り、受け取った暗号化乱数  $S_2$  をメモリカード 200 の通信部 270 へ出力する。

##### 【0040】

通信部 340 は、制御部 350 から通信中止信号を受け取ると、メモリカード 200 の通信部 270 との通信を中止する。

通信部 340 は、暗号部 360 から暗号化部分著作物  $F_i$  ( $i = 1, 2, 3, \dots$ ) を受け取り、受け取った暗号化部分著作物  $F_i$  ( $i = 1, 2, 3, \dots$ ) をメモリカード 200 の通信部 270 へ出力する。

#### 1. 2. 10 制御部 350



制御部 350 は、相互認証制御部 334 からメモリカードライタ 300 に装着されたメモリカード 200 が正しい装置であるか、不正な装置であることを示す認証信号を受け取る。

【0041】

制御部 350 は、受け取った認証信号が不正な装置であることを示す場合には、メモリカード 200 との通信を中止する通信中止信号を通信部 340 へ出力する。

制御部 350 は、受け取った認証信号が正しい装置であることを示す場合には、著作物取得部 380 に対して、外部からの著作物取得を指示する著作物取得信号を出力する。

1. 2. 11 著作物取得部 380

著作物取得部 380 は、制御部 350 から著作物取得信号を受け取る。

【0042】

著作物取得部 380 は、制御部 350 から著作物取得信号を受け取ると、通信回線 10 を経由して、外部から音楽の著作物を取得し、取得した著作物を著作物記憶部 370 へ出力する。

1. 2. 12 著作物記憶部 370

著作物記憶部 370 は、著作物取得部 380 から著作物を受け取り、受け取った著作物を記憶する。

1. 2. 13 暗号部 360

暗号部 360 は、著作物記憶部 370 から著作物を読み出し、メディア固有鍵記憶部 323 から固有鍵  $K' i$  を読み出す。

【0043】

暗号部 360 は、DES により規格されている暗号アルゴリズム E2 をあらかじめ記憶している。

暗号部 360 は、読み出した著作物を複数の 64 ビットのビット列からなる部

分著作物 $C_i$  ( $i = 1, 2, 3, \dots$ )に分割し、各部分著作物 $C_i$  ( $i = 1, 2, 3, \dots$ )に暗号アルゴリズム $E_2$ を施して複数の暗号化部分著作物 $F_i$  ( $i = 1, 2, 3, \dots$ )を生成する。このとき、前記読み出した固有鍵 $K'_i$ を暗号アルゴリズム $E_2$ の鍵とする。生成された暗号化部分著作物 $F_i$  ( $i = 1, 2, 3, \dots$ )は式15に示すように表現できる。

$$(式15) \quad F_i = E_2(K'_i, C_i) \quad (i = 1, 2, 3, \dots)$$

暗号部360は、生成した暗号化部分著作物 $F_i$  ( $i = 1, 2, 3, \dots$ )を通信部340へ出力する。

### 1. 3 メモリカードリーダー400の構成

メモリカードライタ300は、図6に示すように、装置鍵記憶部410、変換部411、装置鍵情報記憶部412、マスタ鍵記憶部413、メディア固有鍵情報記憶部420、逆変換部421、メディア固有鍵記憶部423、相互認証部430、通信部440、制御部450、復号部460、著作物記憶部470、再生部480、操作部490から構成される。

#### 【0044】

装置鍵記憶部410、変換部411、装置鍵情報記憶部412、マスタ鍵記憶部413、メディア固有鍵情報記憶部420、逆変換部421、メディア固有鍵記憶部423、相互認証部430、通信部440、制御部450については、それぞれメモリカードリーダー400の装置鍵記憶部310、変換部311、装置鍵情報記憶部312、マスタ鍵記憶部313、メディア固有鍵情報記憶部320、逆変換部321、メディア固有鍵記憶部323、相互認証部330、通信部340、制御部350と同等であるので、同等部分の説明は省略し、異なる機能、作用を有する点を中心として説明する。

#### 1. 3. 1 制御部450

制御部450は、受け取った認証信号が正しい装置であることを示す場合には、復号部460に対して、通信部440から出力される暗号化著作物の復号を指示する復号指示を出力する。

### 1. 3. 2 復号部 460

復号部 460 は、制御部 450 から復号指示を受け取る。

【0045】

復号部 460 は、制御部 450 から復号指示を受け取ると、通信部 440 から暗号化著作物を受け取り、メディア固有鍵記憶部 423 から固有鍵  $K' i$  を読み出す。

復号部 460 は、DES により規格されている復号アルゴリズム D2 をあらかじめ記憶している。

【0046】

復号部 460 は、受け取った暗号化著作物を複数の 64 ビットのビット列からなる部分暗号化著作物  $G_i$  ( $i = 1, 2, 3, \dots$ ) に分割し、各部分暗号化著作物  $G_i$  ( $i = 1, 2, 3, \dots$ ) に復号アルゴリズム D2 を施して複数の部分著作物  $H_i$  ( $i = 1, 2, 3, \dots$ ) を生成する。このとき、前記読み出した固有鍵  $K' i$  を復号アルゴリズム D2 の鍵とする。生成された部分著作物  $H_i$  ( $i = 1, 2, 3, \dots$ ) は式 16 に示すように表現できる。

$$(式 16) \quad H_i = D2(K' i, G_i) \quad (i = 1, 2, 3, \dots)$$

復号部 460 は、生成した部分著作物  $H_i$  ( $i = 1, 2, 3, \dots$ ) を著作物記憶部 470 へ出力する。

### 1. 3. 3 著作物記憶部 470

著作物記憶部 470 は、復号部 460 から部分著作物  $H_i$  ( $i = 1, 2, 3, \dots$ ) を受け取り、受け取った部分著作物  $H_i$  ( $i = 1, 2, 3, \dots$ ) を記憶する。

### 1. 3. 4 操作部 490

操作部 490 は、各種のユーザの指示を受け付ける複数の操作ボタンを有している。

【0047】

各種のユーザの指示に対応する操作ボタンが、ユーザにより操作されると、操作された操作ボタンに対応する指示を再生部 480 に出力する。

### 1. 3. 5 再生部 480

再生部 480 は、操作部 490 から指示を受け取る。

【0048】

再生部 480 は、受け取った指示に基づいて、著作物記憶部 470 に記憶されている音楽の著作物を読み出し、読み出した著作物を再生する。

## 2. デジタル著作物保護システム 100 の動作

デジタル著作物保護システム 100 の動作について説明する。

### 2. 1 メモリカード 200 がメモリカードライター 300 に装着された場合の概要動作

メモリカード 200 が、メモリカードライター 300 に装着された場合の概要動作について、図 7 に示すフローチャートを用いて説明する。

【0049】

メモリカード 200 が、メモリカードライター 300 に装着されると、メモリカードライター 300 がメモリカード 200 を認証し（ステップ S110）、メモリカードライター 300 が、メモリカード 200 は不正な装置であると認識した場合には（ステップ S111）、メモリカードライター 300 とメモリカード 200 との間で通信を行わず、処理を終了する。

【0050】

メモリカードライター 300 が、メモリカード 200 は正しい装置であると認識した場合には（ステップ S111）、メモリカード 200 がメモリカードライター 300 を認証し（ステップ S112）、メモリカード 200 が、メモリカードライター 300 は不正な装置であると認識した場合には（ステップ S113）、メモリカードライター 300 とメモリカード 200 との間で通信を行わず、処理を終了する。

【0051】

メモリカード200が、メモリカードライター300は正しい装置であると認識した場合には（ステップS113）、メモリカードライター300は、外部から著作物を取得し、取得した著作物を暗号化し、メモリカード200へ出力し（ステップS114）、メモリカード200は、暗号化された著作物を記憶する（ステップS115）。

2. 2 メモリカード200がメモリカードリーダー400に装着された場合の概要動作

メモリカード200が、メモリカードリーダー400に装着された場合の概要動作について、図8に示すフローチャートを用いて説明する。

【0052】

メモリカード200が、メモリカードリーダー400に装着されると、メモリカードリーダー400がメモリカード200を認証し（ステップS120）、メモリカードリーダー400が、メモリカード200は不正な装置であると認識した場合には（ステップS121）、メモリカードリーダー400とメモリカード200との間で通信を行わず、処理を終了する。

【0053】

メモリカードリーダー400が、メモリカード200は正しい装置であると認識した場合には（ステップS121）、メモリカード200がメモリカードリーダー400を認証し（ステップS122）、メモリカード200が、メモリカードリーダー400は不正な装置であると認識した場合には（ステップS123）、メモリカードリーダー400とメモリカード200との間で通信を行わず、処理を終了する。

【0054】

メモリカード200が、メモリカードリーダー400は正しい装置であると認識した場合には（ステップS123）、メモリカード200は、暗号化された著作物をメモリカードリーダー400へ出力し（ステップS124）、メモリカードリ

ーダ400は、メモリカード200から出力された暗号された著作物を復号し（ステップS125）、メモリカードリーダー400は復号された著作物を再生する（ステップS126）。

## 2.3 メモリカード200がメモリカードライター300に装着された場合の詳細の認証動作

メモリカード200が、メモリカードライター300に装着された場合の詳細の認証動作について、図9及び図10を用いて説明する。

### 【0055】

変換部230は、マスタ鍵 $M_k$ を暗号アルゴリズム $E_1$ の鍵として、固有鍵 $K_i$ に暗号アルゴリズム $E_1$ を施して暗号化固有鍵 $E_1(M_k, K_i)$ を生成し（ステップS130）、通信部270は、暗号化固有鍵 $E_1(M_k, K_i)$ を通信部340を経由して逆変換部321へ出力し（ステップS131）、逆変換部321は、マスタ鍵 $M_k$ を復号アルゴリズム $D_1$ の鍵として、暗号化固有鍵 $E_1(M_k, K_i)$ に復号アルゴリズム $D_1$ を施して固有鍵 $K'_i = D_1(M_k, E_1(M_k, K_i))$ を生成し（ステップS132）、乱数発生部331は、乱数 $R_1$ を生成し（ステップS133）、通信部340は、生成された乱数 $R_1$ を通信部270を経由して暗号部252へ出力し（ステップS134）、暗号部252は、固有鍵 $K_i$ を暗号アルゴリズム $E_2$ の鍵として、乱数 $R_1$ に暗号アルゴリズム $E_2$ を施して暗号化乱数 $E_2(K_i, R_1)$ を生成し（ステップS135）、通信部270は、通信部340を経由して暗号化乱数 $E_2(K_i, R_1)$ を復号部333へ出力し（ステップS136）、復号部333は、固有鍵 $K'_i$ を復号アルゴリズム $D_2$ の鍵として、暗号化乱数 $E_2(K_i, R_1)$ に復号アルゴリズム $D_2$ を施して、 $D_2(K'_i, E_2(K_i, R_1))$ を生成し（ステップS137）、相互認証制御部334は、乱数 $R_1$ と $D_2(K'_i, E_2(K_i, R_1))$ とを比較し、一致していれば、メモリカード200は正しい装置であると認識し、一致していなければ、メモリカード200は不正な装置であると認識する（ステップS138）。

### 【0056】

変換部 311 は、マスタ鍵  $M_k$  を暗号アルゴリズム  $E_3$  の鍵として、装置鍵  $A_j$  に暗号アルゴリズム  $E_3$  を施して暗号化装置鍵  $E_3 (M_k, A_j)$  を生成し（ステップ S139）、通信部 340 は、暗号化装置鍵  $E_3 (M_k, A_j)$  を通信部 270 を経由して逆変換部 222 へ出力し（ステップ S140）、逆変換部 222 は、マスタ鍵  $M_k$  を復号アルゴリズム  $D_3$  の鍵として、暗号化装置鍵  $E_3 (M_k, A_j)$  に復号アルゴリズム  $D_3$  を施して装置鍵  $A'_j = D_3 (M_k, E_3 (M_k, A_j))$  を生成し（ステップ S141）、乱数発生部 251 は、乱数  $R_2$  を生成し（ステップ S142）、通信部 270 は、生成された乱数  $R_2$  を通信部 340 を経由して暗号部 332 へ出力し（ステップ S143）、暗号部 332 は、装置鍵  $A_j$  を暗号アルゴリズム  $E_2$  の鍵として、乱数  $R_2$  に暗号アルゴリズム  $E_2$  を施して暗号化乱数  $E_2 (A_j, R_2)$  を生成し（ステップ S144）、通信部 340 は、通信部 270 を経由して暗号化乱数  $E_2 (A_j, R_2)$  を復号部 253 へ出力し（ステップ S145）、復号部 253 は、装置鍵  $A'_j$  を復号アルゴリズム  $D_2$  の鍵として、暗号化乱数  $E_2 (A_j, R_2)$  に復号アルゴリズム  $D_2$  を施して、 $D_2 (A'_j, E_2 (A_j, R_2))$  を生成し（ステップ S146）、相互認証制御部 254 は、乱数  $R_2$  と  $D_2 (A'_j, E_2 (A_j, R_2))$  とを比較し、一致していれば、メモリカードライタ 300 は正しい装置であると認識し、一致していなければ、メモリカードライタ 300 は不正な装置であると認識する（ステップ S147）。

### 3. その他の実施の形態

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は上記の実施の形態に限定されないのはもちろんである。すなわち、以下のような場合も本発明に含まれる。

#### 3. 1 デジタル著作物保護システム 100a

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム 100a は、図 11 のブロック図に示すように、メモリカード 200a、メディ

ア固有鍵情報作成装置 600、メモリカードライタ 300、メモリカードリーダー 400 から構成される。

【0057】

メモリカードライタ 300、メモリカードリーダー 400 は、それぞれデジタル著作物保護システム 100 のメモリカードライタ 300、メモリカードリーダー 400 とほぼ同様であるので、説明は省略する。

メモリカード 200 a は、メディア固有鍵情報作成装置 600 と接続される。

3. 1. 1 メディア固有鍵情報作成装置 600

メディア固有鍵情報作成装置 600 は、マスタ鍵記憶部 210 b、メディア固有鍵記憶部 220 b、変換部 230 b、メディア固有鍵情報記憶部 240 b、通信部 270 b から構成される。

【0058】

マスタ鍵記憶部 210 b、メディア固有鍵記憶部 220 b、変換部 230 b、メディア固有鍵情報記憶部 240 b については、それぞれメモリカード 200 のマスタ鍵記憶部 210、メディア固有鍵記憶部 220、変換部 230、メディア固有鍵情報記憶部 240 と同様の機能、作用、構成を有しており、以下においてはそれぞれの相違点を中心にして説明する

(1) マスタ鍵記憶部 210 b

マスタ鍵記憶部 210 b は、マスタ鍵記憶部 210 と同様にあらかじめ一つのマスタ鍵  $M_k$  を記憶している。

(2) メディア固有鍵記憶部 220 b

メディア固有鍵記憶部 220 b は、通信部 270 b から固有鍵  $K_i$  を受け取り、受け取った固有鍵  $K_i$  を記憶する。

(3) 変換部 230 b

変換部 230 b は、変換部 230 と同様にして、メディア固有鍵記憶部 220



bに記憶されている固有鍵Kiとマスタ鍵記憶部210aに記憶されているマスタ鍵Mkを用いて、暗号化固有鍵Jiを生成し、生成した暗号化固有鍵Jiをメディア固有鍵情報記憶部240bへ出力する。

(4) メディア固有鍵情報記憶部240b

メディア固有鍵情報記憶部240bは、変換部230bから、暗号化固有鍵Jiを受け取り、受け取った暗号化固有鍵Jiを記憶する。

(5) 通信部270b

通信部270bは、メモリカード200aの通信部270aから固有鍵Kiを受け取り、受け取った固有鍵Kiをメディア固有鍵記憶部220bへ出力する。

【0059】

通信部270bは、メディア固有鍵情報記憶部240bから暗号化固有鍵Jiを読み出し、読み出した暗号化固有鍵Jiをメモリカード200aの通信部270aへ出力する。

3. 1. 2 メモリカード200a

メモリカード200aは、この図に示すように、マスタ鍵記憶部210、メディア固有鍵記憶部220、メディア固有鍵情報記憶部240a、装置鍵記憶部221、逆変換部222、装置鍵情報記憶部223、相互認証部250、暗号化著作物記憶部260、通信部270a、制御部280から構成される。

【0060】

メモリカード200aのマスタ鍵記憶部210、メディア固有鍵記憶部220、装置鍵記憶部221、逆変換部222、装置鍵情報記憶部223、相互認証部250、暗号化著作物記憶部260、制御部280は、それぞれ、メモリカード200aのマスタ鍵記憶部210、メディア固有鍵記憶部220、装置鍵記憶部221、逆変換部222、装置鍵情報記憶部223、相互認証部250、暗号化著作物記憶部260、制御部280と同じであるので説明を省略し、メモリカード200aのメディア固有鍵情報記憶部240a、通信部270aについて、メモ

リカード 200 のメディア固有鍵情報記憶部 240、通信部 270 との相違点を中心にして説明する。

(1) メディア固有鍵情報記憶部 240 a

メディア固有鍵情報記憶部 240 a は、通信部 270 a から暗号化固有鍵  $J_i$  を受け取り、受け取った暗号化固有鍵  $J_i$  を記憶する。

(2) 通信部 270 a

通信部 270 a は、メディア固有鍵記憶部 220 から固有鍵  $K_i$  を読み出し、読み出した固有鍵  $K_i$  をメディア固有鍵情報作成装置 600 の通信部 270 b へ出力する。

【0061】

通信部 270 a は、メディア固有鍵情報作成装置 600 の通信部 270 b から暗号化固有鍵  $J_i$  を受け取り、受け取った暗号化固有鍵  $J_i$  をメディア固有鍵情報記憶部 240 a へ出力する。

3. 1. 3 メモリカード 200 a がメモリカードライター 300 に装着された場合の詳細の認証動作

メモリカード 200 a が、メモリカードライター 300 に装着された場合の詳細の認証動作について、図 9 との相違点につき、図 12 を用いて説明する。

【0062】

認証動作の詳細は、図 9 に示すステップ S139～S147 が、図 12 に示すステップ S201～S206 に置き換えられたものとなる。

乱数発生部 251 は、乱数  $R_3$  を生成し（ステップ S201）、通信部 270 a は、生成された乱数  $R_3$  を通信部 340 を経由して暗号部 332 へ出力し（ステップ S202）、暗号部 332 は、マスタ鍵  $M_k$  を暗号アルゴリズム E2 の鍵として、乱数  $R_3$  に暗号アルゴリズム E2 を施して暗号化乱数 E2 ( $M_k$ 、 $R_3$ ) を生成し（ステップ S203）、通信部 340 は、通信部 270 を経由して暗号化乱数 E2 ( $M_k$ 、 $R_3$ ) を復号部 253 へ出力し（ステップ S204）、復

号部 253 は、マスタ鍵  $M_k$  を復号アルゴリズム  $D_2$  の鍵として、暗号化乱数  $E_2$  ( $M_k$ 、 $R_3$ ) に復号アルゴリズム  $D_2$  を施して、 $D_2$  ( $M_k$ 、 $E_2$  ( $M_k$ 、 $R_3$ )) を生成し (ステップ S205)、相互認証制御部 254 は、乱数  $R_3$  と  $D_2$  ( $M_k$ 、 $E_2$  ( $M_k$ 、 $R_3$ )) とを比較し、一致していれば、メモリカードライタ 300 は正しい装置であると認識し、一致していなければ、メモリカードライタ 300 は不正な装置であると認識する (ステップ S206)。

### 3. 1. 4 まとめ

この実施の形態によると、メモリカード 200a が使用者に配布、販売される前に、メモリカード 200a とメディア固有鍵情報作成装置 600 とが接続され、メディア固有鍵情報作成装置 600 により生成された暗号化固有鍵  $J_i$  がメモリカード 200a に書き込まれる。

#### 【0063】

このように構成することにより、メモリカード 200 から、変換部 230 を取り去ることができ、メモリカード 200a では、メモリカード 200 と比較して回路規模を小さくできるという効果がある。

### 3. 2 別のデジタル著作物保護システム

デジタル著作物保護システム 100 では、メモリカード 200、メモリカードライタ 300、メモリカードリーダー 400 は、同一のマスタ鍵を有し、マスタ鍵を共通鍵暗号アルゴリズム又は共通鍵復号アルゴリズムの鍵としているが、マスタ鍵の代わりに、メモリカード 200 は公開鍵暗号の一種である RSA 暗号の公開鍵  $K_p$  を有し、メモリカードライタ 300、メモリカードリーダー 400 は、その秘密鍵  $K_s$  を有するとしてもよい。

#### 【0064】

ここで、公開鍵  $K_p$  と秘密鍵  $K_s$  は、次のようにして決定される。 $p$ 、 $q$  をそれぞれ約 160 桁程度の 10 進数とし、その積を  $n$  とし、整数  $L$  を  $p-1$  及び  $q-1$  の最小公倍数とし、数  $e$  及び  $d$  を法  $L$  の下で互いに逆数となる数とする。すなわち、 $e \cdot d = 1 \pmod{L}$  とする。また、公開鍵  $K_p$  を  $n$  及び  $e$  とし、

秘密鍵  $K_s$  を  $d$  とする。変換部においては、入力  $M$  に対して法  $n$  の下で  $M^e$  ( $M$  の  $e$  乗) の演算を行って変換結果  $C$  を求め、逆変換部においては、入力  $C$  に対して  $C^d$  ( $C$  の  $d$  乗) の演算を行う。法  $n$  の下で  $C^d = (M^e)^d = M^{ed} = M$  であるから首尾よく逆変換ができることが分かる。

【0065】

公開鍵  $K_p$  は、上記に示すようにしてあらかじめ別の公開鍵生成装置により生成され、生成された公開鍵  $K_p$  がメモリカード 200 に送信されている。

(メモリカード 200 がメモリカードライター 300 に装着された場合の詳細の認証動作)

次に、メモリカード 200 がメモリカードライター 300 に装着された場合の詳細の認証動作について図 13 を用いて説明する。なお、図 10 と同じ符号を有するステップについては、同じ動作であるので説明を省略する。

【0066】

公開鍵生成装置は、あらかじめメモリカードライター 300 から秘密鍵  $K_s$  を読み出し、読み出した秘密鍵  $K_s$  を基にして公開鍵暗号アルゴリズムを用いて、公開鍵  $K_p$  を生成し、生成した公開鍵  $K_p$  をメモリカード 200 に送信し、メモリカード 200 は送信された公開鍵  $K_p$  を記憶する (ステップ S301)。

変換部 230 は、公開鍵  $K_p$  を暗号アルゴリズム  $E4$  の鍵として、固有鍵  $K_i$  に暗号アルゴリズム  $E4$  を施して暗号化固有鍵  $E4(K_p, K_i)$  を生成し (ステップ S302)、通信部 270 は、暗号化固有鍵  $E4(K_p, K_i)$  を通信部 340 を経由して逆変換部 321 へ出力し (ステップ S303)、逆変換部 321 は、秘密鍵  $K_s$  を復号アルゴリズム  $D4$  の鍵として、暗号化固有鍵  $E4(K_p, K_i)$  に復号アルゴリズム  $D4$  を施して固有鍵  $K'_i = D4(K_s, E4(K_p, K_i))$  を生成する (ステップ S304)。

【0067】

なお、暗号アルゴリズム  $E4$  及び復号復号アルゴリズム  $D4$  は楕円暗号によるアルゴリズムである。

公開鍵と秘密鍵がこのように構成されているため、秘密鍵  $d$  から公開鍵  $e$  を計算できない。なぜならば、秘密鍵  $d$  が分かっているとき、これから  $e$  を求めるた

めには法  $L$  が知られていなければならないが、 $L$  は  $p-1$  と  $q-1$  の最小公倍数であるため、 $p$  と  $q$  との積を知っているだけでは求められないからである。このことにより、カードリーダー又はカードライターに存在する秘密鍵  $d$  が仮に暴露されたとしてもこれから公開鍵  $e$  を求めることができないので、メモリカードの偽造が困難であるという効果がある。

### 3. 3 別のデジタル著作物保護システム

上記の「3. 2 別のデジタル著作物保護システム」に示すデジタル著作物保護システムでは、メモリカード 200 は公開鍵  $K_p$  を有し、メモリカードライター 300、メモリカードリーダー 400 は、秘密鍵  $K_s$  を有するとしているが、また別のデジタル著作物保護システムにおいては、メモリカード 200 は、公開鍵暗号系的一种である楕円曲線上の回復型署名の秘密鍵  $K_s$  を有し、メモリカードライター 300、メモリカードリーダー 400 は、公開鍵  $K_p$  を有するとしてもよい。ここで、公開鍵  $K_p$  と秘密鍵  $K_s$  は次のようにして決定される。

【0068】

秘密鍵  $K_s$  としてスカラー  $x$  が選ばれる。公開鍵  $K_p$  は、楕円曲線上の基点を  $G$  とし、 $G + G + \dots + G$  ( $x$  回の加算) の点とする。変換処理として秘密鍵  $K_s$  を用いた回復型署名変換を用い、逆変換処理として公開鍵  $K_p$  を用いて回復型署名検証変換を用いる。なお、回復型署名については、「A message recovery signature scheme equivalent to DSA over elliptic curves」(Atsuko Miyaji 著、Advances in Cryptology- Proceedings of ASIACRYPT'96, Lecture Notes in Computer Science, 1163(1996), Springer-Verlag, 1-14) に記載されているので、説明は省略する。

【0069】

このとき、公開鍵  $K_p$  は、メモリカード 200 が有する秘密鍵  $K_s$  を基にして公開鍵暗号アルゴリズムを用いて、あらかじめ別の公開鍵生成装置により生成され、生成された公開鍵  $K_p$  がメモリカードライター 300 に送信されている。

変換部 230 は、秘密鍵  $K_s$  を暗号アルゴリズム  $E_4$  の鍵として、固有鍵  $K_i$  に暗号アルゴリズム  $E_4$  を施して暗号化固有鍵  $E_4(K_s, K_i)$  を生成する。

また、逆変換部 321 は、公開鍵  $K_p$  を復号アルゴリズム  $D_4$  の鍵として、暗号化固有鍵  $E_4 (K_s, K_i)$  に復号アルゴリズム  $D_4$  を施して固有鍵  $K'_i = D_4 (K_p, E_4 (K_s, K_i))$  を生成する。

【0070】

公開鍵  $K_p$  と秘密鍵  $K_s$  がこのように構成されているので、公開鍵  $K_p$  から秘密鍵  $K_s$  を求めることが、計算量的に非常に困難となる。従って、メモリカードに比べて内部解析の危険性が相対的に高いと思われるメモリライタ又はメモリリーダーに公開鍵を与え、メモリカードに秘密鍵を与える構成が、全体のセキュリティを高める効果を持つ。

【0071】

なお、楕円曲線暗号系のような離散対数問題に安全性の根拠を持つ公開鍵暗号系では、秘密鍵から公開鍵が求められることに注意されたい。

### 3. 4 別のデジタル著作物保護システム

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム 100c は、図 14、図 15、図 16 のブロック図にそれぞれ示すメモリカード 200c、メモリカードライタ 300c、メモリカードリーダー 400c から構成される。

【0072】

メモリカード 200c は、図示していないマスタ鍵選択装置に装着される。また、メモリカードライタ 300c、メモリカードリーダー 400c は、マスタ鍵選択装置に接続される。

#### 3. 4. 1 マスタ鍵選択装置

マスタ鍵選択装置にメモリカード 200c が装着される場合には、マスタ鍵選択装置は、メモリカード 200c の通信部 270 と接続される。

【0073】

マスタ鍵選択装置とメモリカードライタ 300c とが接続される場合には、マスタ鍵選択装置は、メモリカードライタ 300c の通信部 340 と接続される。

マスタ鍵選択装置とメモリカードリーダー 400c とが接続される場合には、マスタ鍵選択装置は、メモリカードリーダー 400c の通信部 440 と接続される。

マスタ鍵選択装置は、メモリカード 200c、メモリカードライター 300c 又はメモリカードリーダー 400c と接続される場合に、接続されるメモリカード 200c の通信部 270、メモリカードライター 300c の通信部 340 又はメモリカードリーダー 400c の通信部 440 に対してパスワードを出力する。

【0074】

パスワードは、複数のマスタ鍵のうちの一つに対応する。

3. 4. 2 メモリカード 200c

メモリカード 200c は、メモリカード 200 にさらにマスタ鍵選択部 215 を備える。メモリカード 200c のその他の構成要素は、メモリカード 200 と同様である。以下において、メモリカード 200 との相違点を中心にして説明する。

【0075】

マスタ鍵記憶部 210 は、複数のマスタ鍵をあらかじめ記憶している。

メモリカード 200c がマスタ鍵選択装置に装着されたとき、メモリカード 200c は、マスタ鍵選択装置と通信部 270 を介して接続される。

通信部 270 は、マスタ鍵選択装置からパスワードを受け取り、受け取ったパスワードをマスタ鍵選択部 215 に出力する。

【0076】

マスタ鍵選択部 215 は、通信部 271 から受け取ったパスワードを用いて、対応する一つのマスタ鍵をマスタ鍵記憶部 210 から選択し、選択したマスタ鍵をマスタ鍵記憶部 210 へ出力する。

マスタ鍵記憶部 210 は、選択されたマスタ鍵に選択されたことを示す選択マークを付し、記憶する。

【0077】

変換部 203、逆変換部 222 は、前記選択マークを付されたマスタ鍵を読み出す。

### 3. 4. 3 メモリカードライタ 300c、メモリカードリーダー 400c

メモリカードライタ 300c は、メモリカードライタ 300 にさらにマスタ鍵選択部 315 を備える。メモリカードライタ 300c のその他の構成要素は、メモリカードライタ 300 と同様である。

#### 【0078】

マスタ鍵記憶部 313 は、複数のマスタ鍵をあらかじめ記憶している。

メモリカード 200c と同様に、通信部 340 はマスタ鍵選択装置からパスワードを受け取り、マスタ鍵選択部 315 に出力し、マスタ鍵選択部 315 は、受け取ったパスワードを用いて、対応する一つのマスタ鍵をマスタ鍵記憶部 313 から選択し、マスタ鍵記憶部 313 は、選択されたマスタ鍵に選択されたことを示す選択マークを付し、記憶する。

#### 【0079】

変換部 311、逆変換部 321 は、前記選択マークを付されたマスタ鍵を読み出す。

メモリカードリーダー 400c についても、メモリカードライタ 300c と同様である。

### 3. 4. 4 まとめ

本実施の形態が適用される望ましい運用形態においては、運用システムの規格を決定すると同時にマスタ鍵などの秘密情報の秘密性を確保する立場にあり、各製造業者にライセンスの許諾を与えるライセンス組織と、ライセンス組織より許諾を受け、所定の規格の機器を製造し、ユーザに提供する立場にある製造業者と、個々の機器を利用するユーザとの 3 者が存在する。メモリカード用のマスタ鍵選択装置 901 とメモリカードライタ用のマスタ鍵選択装置 902 とメモリカードリーダー用のマスタ鍵選択装置 903 とのうち、マスタ鍵選択装置 901 は製造業者の手元にあり、マスタ鍵選択装置 902 とマスタ鍵選択装置 903 とはライセンス組織の手元にあって、製造業者には渡されない。

#### 【0080】



従って、製造業者が製造する装置の運用状態においては、メモリカードは複数のマスタ鍵を有しており、そのうちの一つをマスタ鍵選択装置 901 により選択する。一方、メモリカードライター又はメモリカードリーダーには、予めライセンス組織がマスタ鍵選択装置 901 又は 902 を用いて選択した結果のマスタ鍵だけが記録されている。

#### 【0081】

マスタ鍵は運用システム毎に選ばれる。例えば、A 社、B 社、C 社の 3 者が共同で運営する音楽配信システムには、マスタ鍵 Mk1 が用いられ、X 社、Y 社、Z 社が共同で運営する映画レンタルシステムにはマスタ鍵 Mk2 が用いられる。

このように、装置の製造に当たって厳重なセキュリティ条件を課することが困難なため、異なる運用システムに異なるマスタ鍵が用いられるので、メモリカードよりも相対的に解析が容易と思われるメモリカードライター又はメモリカードリーダーを運用システム毎に特化することにより、ある運用システムのマスタ鍵の暴露が他の運用システムに影響を与えない、安全性の高いセキュリティシステムを実現できるという効果がある。

### 3. 5 その他の変形例

(1) 上記の実施の形態においては、デジタル著作物保護システムは、メモリカードとメモリメモリカードライターとメモリカードリーダーとから構成されるとしているが、デジタル著作物保護システムは、メモリカードとメモリカードライターとから構成されるとしてもよい。また、デジタル著作物保護システムは、メモリカードとメモリカードリーダーとから構成されるとしてもよい。

(2) 上記の実施の形態においては、DES 暗号を用いるとしているが他の暗号を用いてもよい。

(3) メモリカードは、半導体メモリの代わりに、光ディスク媒体や MO (M a g n e t o - O p t i c a l) 媒体を有するとしてもよい。

(4) 本発明は、コンピュータにより実行するプログラムを記録したコンピュータ読み取り可能な記録媒体であって、上記手順をコンピュータに実行させるプログラムを記録していることを特徴とする。

(5) また、前記記録媒体を移送することにより、又は、前記プログラムを通信回線を通して移送することにより、独立した他のコンピュータシステムで実施するようにしてもよい。

【0082】

【発明の効果】

上記に説明したように、本発明は、記録媒体とアクセス装置とが接続された状態で、両者間で機器認証フェーズと著作物転送フェーズとを実行して著作物の正当者への配布を実現するデジタル著作物保護システムであって、機器認証フェーズでは、記録媒体が所有する固有鍵をアクセス装置に秘密伝送し、アクセス装置が取得した固有鍵を用いて、機器認証を行い、著作物転送フェーズでは、機器認証が成功した場合にのみ、アクセス装置が取得した固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する。

【0083】

この構成によると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるという効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

また、本発明は、記録媒体とアクセス装置とが接続された状態で、前記記録媒体と前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行うデジタル著作物保護システムであって、前記記録媒体は、記録媒体毎に異なる固有鍵を予め記憶している固有鍵記憶領域と、接続されたアクセス装置へ前記固有鍵を秘密伝送し、前記固有鍵を用いて前記アクセス装置との間で機器認証を行う第1認証手段と、前記固有鍵を用いて暗号化される著作物を保持するための領域とを備え、前記アクセス装置は、記録媒体から秘密伝送された固有鍵を用いて、前記記録媒体との間で機器認証を行う第2認証手段と、機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送手段とを備える。

【0084】

この構成によると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるという効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

ここで、前記第1認証手段は、あらかじめ第1鍵を有し、前記第1鍵を用いて、前記固有鍵に第1暗号を施して暗号化固有鍵を生成して伝送し、前記第2認証手段は、あらかじめ前記第1鍵を有し、前記第1鍵を用いて、前記伝送された暗号化固有鍵に、前記第1暗号の逆変換を行う第1復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【0085】

この構成によると、記録装置とアクセス装置とは同一のマスタ鍵を有するので、記録装置とアクセス装置との製造が容易に行えるという効果がある。

ここで、前記第1認証手段は、第1鍵を基にして、公開鍵暗号方式の公開鍵決定アルゴリズムにより算出された公開鍵である第2鍵をあらかじめ有し、前記第2鍵を用いて、前記固有鍵に第1暗号を施して暗号化固有鍵を生成して伝送し、前記第2認証手段は、あらかじめ前記第1鍵を有し、前記第1鍵を用いて、前記伝送された暗号化固有鍵に、前記第1暗号の逆変換を行う第1復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【0086】

この構成によると、秘密鍵  $d$  から公開鍵  $e$  を計算できない。なぜならば、秘密鍵  $d$  が分かっているとき、これから  $e$  を求めるためには法  $L$  が知られていなければならないが、 $L$  は  $p-1$  と  $q-1$  の最小公倍数であるため、 $p$  と  $q$  との積を知っているだけでは求められないからである。このことにより、カードリーダ又は

カードライタに存在する秘密鍵  $d$  が仮に暴露されたとしてもこれから公開鍵  $e$  を求めることができないので、メモリカードの偽造が困難であるという効果がある。

ここで、前記第 1 認証手段は、あらかじめ第 1 鍵を有し、前記第 1 鍵を用いて、前記固有鍵に回復型署名処理を施して署名文を生成して伝送し、前記第 2 認証手段は、前記第 1 鍵に前記回復型署名処理の公開鍵決定アルゴリズムにより算出された公開鍵である第 2 鍵をあらかじめ有し、前記第 2 鍵を用いて、前記伝送された署名文に、前記回復型署名の検証処理を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

#### 【0087】

この構成によると、公開鍵  $K_p$  から秘密鍵  $K_s$  を求めることが、計算量的に非常に困難となる。従って、メモリカードに比べて内部解析の危険性が相対的に高いと思われるメモリライタ又はメモリリーダーに公開鍵を与え、メモリカードに秘密鍵を与える構成が、全体のセキュリティを高めると言う効果がある。

ここで、前記デジタル著作物保護システムは、さらに固有鍵に第 1 暗号を施して暗号化固有鍵に変換する固有鍵変換手段を備える暗号化固有鍵作成装置を有し、前記第 1 認証手段は、前記固有鍵を前記固有鍵変換手段へ出力して暗号化固有鍵に変換し、変換された暗号化固有鍵を前記アクセス装置へ伝送し、前記第 2 認証手段は、記録媒体から伝送された暗号化固有鍵に前記第 1 暗号の逆処理を行う第 1 復号を施して固有鍵を生成するように構成してもよい。

#### 【0088】

この構成によると、記録媒体は、変換部を有しないので、回路規模を小さくすることができるという効果を有する。

ここで、前記第 1 認証手段は、あらかじめ複数の第 1 鍵を有し、前記複数の第 1 鍵のうち一つの第 2 鍵の選択を受け付け、前記第 2 鍵を用いて、前記固有鍵に

第1暗号を施して暗号化固有鍵を生成して伝送し、前記第2認証手段は、あらかじめ複数の第1鍵を有し、前記複数の第1鍵から前記第2鍵の選択を受け付け、前記第2鍵を用いて、前記伝送された暗号化固有鍵に、前記第1暗号の逆変換を行う第1復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

## 【0089】

この構成によると、記録媒体及びアクセス装置は、複数のマスタ鍵を有しているので、複数の異なるデジタル著作物保護システムにおいても適用ができるという効果がある。

また、本発明は、アクセス装置と接続された状態で、前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行う記録媒体であって、記録媒体毎に異なる固有鍵を記憶している固有鍵記憶領域と、前記固有鍵を用いて暗号化される著作物を保持するための領域と、アクセス装置が接続されたとき、記録媒体から当該アクセス装置へ固有鍵を秘密伝送する手順を経て、当該アクセス装置との間で機器認証を行う認証手段と、機器認証が成功した場合にのみ、前記固有鍵を用いて暗号化された著作物を受け取り前記領域に書き込み若しくは前記領域に記憶されている暗号化された著作物を読み出して前記アクセス装置へ出力する転送手段とを備える。

## 【0090】

この媒体を用いると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるという効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

また、本発明は、固有鍵を有する記録媒体と接続され、前記記録媒体との間で機器認証と暗号化された著作物の転送とを行うアクセス装置であって、記録媒体から固有鍵を秘密伝送される手順を経て、前記記録媒体との間で機器認証を行う

認証手段と、機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送手段とを備える。

【0091】

このアクセス装置を用いると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるという効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

また、本発明は、記録媒体とアクセス装置とが接続された状態で、両者間で機器認証ステップと著作物転送ステップとを実行して著作物の正当者への配布を実現するデジタル著作物保護方法であって、機器認証ステップでは、記録媒体が所有する固有鍵をアクセス装置に秘密伝送し、アクセス装置が取得した固有鍵を用いて、機器認証を行い、著作物転送ステップでは、機器認証が成功した場合にのみ、アクセス装置が取得した固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する。

【0092】

この方法を用いると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるという効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

また、本発明は、記録媒体毎に異なる固有鍵を予め記憶している固有鍵記憶領域及び前記固有鍵を用いて暗号化される著作物を保持するための領域を有する記録媒体とアクセス装置とが接続された状態で、前記記録媒体と前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行うデジタル著作物保護システムで用いられるデジタル著作物保護方法であって、接続されたアクセス装置へ

前記固有鍵を秘密伝送し、前記固有鍵を用いて前記アクセス装置との間で機器認証を行う第1認証ステップと、記録媒体から秘密伝送された固有鍵を用いて、前記記録媒体との間で機器認証を行う第2認証ステップと、機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送ステップとを含む。

### 【0093】

この方法を用いると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるという効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

ここで、前記第1認証ステップは、あらかじめ第1鍵を有し、前記第1鍵を用いて、前記固有鍵に第1暗号を施して暗号化固有鍵を生成して伝送し、前記第2認証ステップは、あらかじめ前記第1鍵を有し、前記第1鍵を用いて、前記伝送された暗号化固有鍵に、前記第1暗号の逆変換を行う第1復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

### 【0094】

この方法を用いると、記録装置とアクセス装置とは同一のマスタ鍵を有するので、記録装置とアクセス装置との製造が容易に行えるという効果がある。

ここで、前記第1認証ステップは、第1鍵を基にして、公開鍵暗号方式の公開鍵決定アルゴリズムにより算出された公開鍵である第2鍵をあらかじめ有し、前記第2鍵を用いて、前記固有鍵に第1暗号を施して暗号化固有鍵を生成して伝送し、前記第2認証ステップは、あらかじめ前記第1鍵を有し、前記第1鍵を用いて、前記伝送された暗号化固有鍵に、前記第1暗号の逆変換を行う第1復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器

認証を行い、前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

#### 【0095】

この方法を用いると、秘密鍵  $d$  から公開鍵  $e$  を計算できない。なぜならば、秘密鍵  $d$  が分かっているとき、これから  $e$  を求めるためには法  $L$  が知られていなければならないが、 $L$  は  $p-1$  と  $q-1$  の最小公倍数であるため、 $p$  と  $q$  との積を知っているだけでは求められないからである。このことにより、カードリーダ又はカードライターに存在する秘密鍵  $d$  が仮に暴露されたとしてもこれから公開鍵  $e$  を求めることができないので、メモリカードの偽造が困難であるという効果がある。

ここで、前記第1認証ステップは、あらかじめ第1鍵を有し、前記第1鍵を用いて、前記固有鍵に回復型署名処理を施して署名文を生成して伝送し、前記第2認証ステップは、前記第1鍵に前記回復型署名処理の公開鍵決定アルゴリズムにより算出された公開鍵である第2鍵をあらかじめ有し、前記第2鍵を用いて、前記伝送された署名文に、前記回復型署名の検証処理を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

#### 【0096】

この方法を用いると、公開鍵  $K_p$  から秘密鍵  $K_s$  を求めることが、計算量的に非常に困難となる。従って、メモリカードに比べて内部解析の危険性が相対的に高いと思われるメモリライター又はメモリリーダに公開鍵を与え、メモリカードに秘密鍵を与える構成が、全体のセキュリティを高めると言う効果がある。

ここで、前記デジタル著作物保護システムは、さらに固有鍵に第1暗号を施して暗号化固有鍵に変換する固有鍵変換手段を備える暗号化固有鍵作成装置を有し、前記第1認証ステップは、前記固有鍵を前記固有鍵変換手段へ出力して暗号化固有鍵に変換し、変換された暗号化固有鍵を前記アクセス装置へ伝送し、前記第2認証ステップは、記録媒体から伝送された暗号化固有鍵に前記第1暗号の逆処



理を行う第1復号を施して固有鍵を生成するように構成してもよい。

【0097】

この方法を用いると、記録媒体は、変換部を有しないので、回路規模を小さくすることができるという効果を有する。

ここで、前記第1認証ステップは、あらかじめ複数の第1鍵を有し、前記複数の第1鍵のうち一つの第2鍵の選択を受け付け、前記第2鍵を用いて、前記固有鍵に第1暗号を施して暗号化固有鍵を生成して伝送し、前記第2認証ステップは、あらかじめ複数の第1鍵を有し、前記複数の第1鍵から前記第2鍵の選択を受け付け、前記第2鍵を用いて、前記伝送された暗号化固有鍵に、前記第1暗号の逆変換を行う第1復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【0098】

この方法を用いると、記録媒体及びアクセス装置は、複数のマスタ鍵を有しているので、複数の異なるデジタル著作物保護システムにおいても適用ができるという効果がある。

また、本発明は、以上に説明したデジタル著作物保護方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体であり、前記プログラムにより上記方法をコンピュータに実行させることにより、上記デジタル著作物保護システムと同様の効果を奏することは明らかである。

【図面の簡単な説明】

【図1】

本発明に係る一つの実施の形態としてのデジタル著作物保護システム100のブロック図を示す。

【図2】

メモ리카ード200がメモ리카ードライター300に装着され、メモ리카ードライター300がパーソナルコンピュータ500に装着される状態を示す。

【図 3】

メモリカード 200 がメモリカードリーダー 400 の一種であるヘッドホンステレオ 401 に装着される状態を示す。

【図 4】

メモリカード 200 の構成を示すブロック図である。

【図 5】

メモリカードライター 300 の構成を示すブロック図である。

【図 6】

メモリカードリーダー 400 の構成を示すブロック図である。

【図 7】

メモリカード 200 が、メモリカードライター 300 に装着された場合の概要動作を示すフローチャートである。

【図 8】

メモリカード 200 が、メモリカードリーダー 400 に装着された場合の概要動作を示すフローチャートである。

【図 9】

メモリカード 200 が、メモリカードライター 300 に装着された場合の詳細の認証動作を示す。

【図 10】

メモリカード 200 が、メモリカードライター 300 に装着された場合の詳細の認証動作を示す。

【図 11】

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム 100a の構成を示すブロック図である。

【図 12】

メモリカード 200a が、メモリカードライター 300 に装着された場合の詳細の認証動作を示す。

【図 13】

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム

において、メモリカード 200 がメモリカードライター 300 に装着された場合の詳細の認証動作を示す。

【図 14】

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム 100c におけるメモリカード 200c の構成を示すブロック図である。

【図 15】

デジタル著作物保護システム 100c におけるメモリカードライター 300c の構成を示すブロック図である。

【図 16】

デジタル著作物保護システム 100c におけるメモリカードリーダー 400c の構成を示すブロック図である。

【符号の説明】

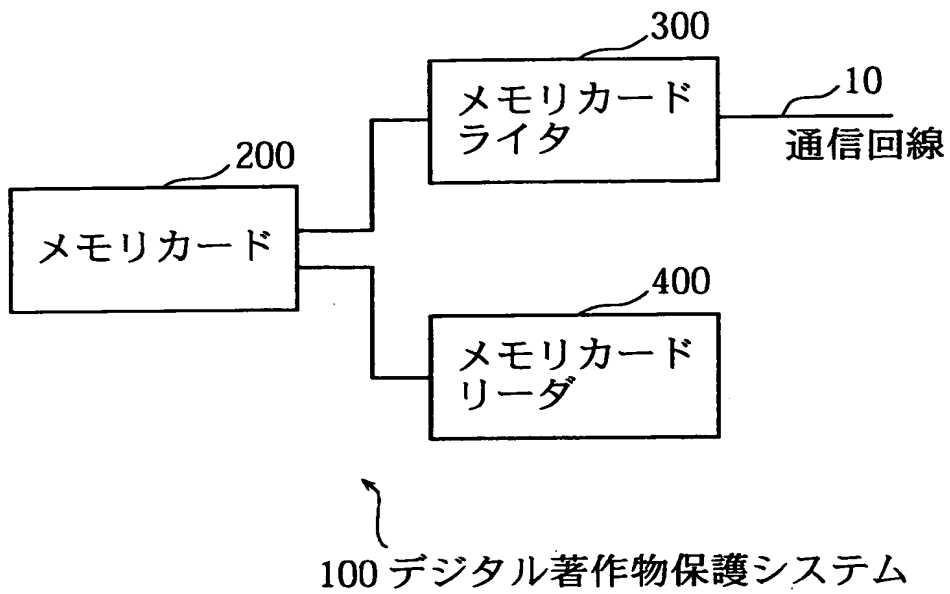
- 10 通信回線
- 100 デジタル著作物保護システム
- 200 メモリカード
- 210 マスタ鍵記憶部
- 220 メディア固有鍵記憶部
- 221 装置鍵記憶部
- 222 逆変換部
- 223 装置鍵情報記憶部
- 230 変換部
- 240 メディア固有鍵情報記憶部
- 250 相互認証部
- 251 乱数発生部
- 252 暗号部
- 253 復号部
- 254 相互認証制御部 254
- 260 暗号化著作物記憶部
- 270 通信部

- 280 制御部
- 300 メモリカードライタ
- 310 装置鍵記憶部
- 311 変換部
- 312 装置鍵情報記憶部
- 313 マスタ鍵記憶部
- 320 メディア固有鍵情報記憶部
- 321 逆変換部
- 323 メディア固有鍵記憶部
- 330 相互認証部
- 331 乱数発生部
- 332 暗号部
- 333 復号部
- 334 相互認証制御部
- 340 通信部
- 350 制御部
- 360 暗号部
- 370 著作物記憶部
- 380 著作物取得部
- 400 メモリカードリーダー
- 410 装置鍵記憶部
- 411 変換部
- 412 装置鍵情報記憶部
- 413 マスタ鍵記憶部
- 420 メディア固有鍵情報記憶部
- 421 逆変換部
- 423 メディア固有鍵記憶部
- 430 相互認証部
- 431 乱数発生部

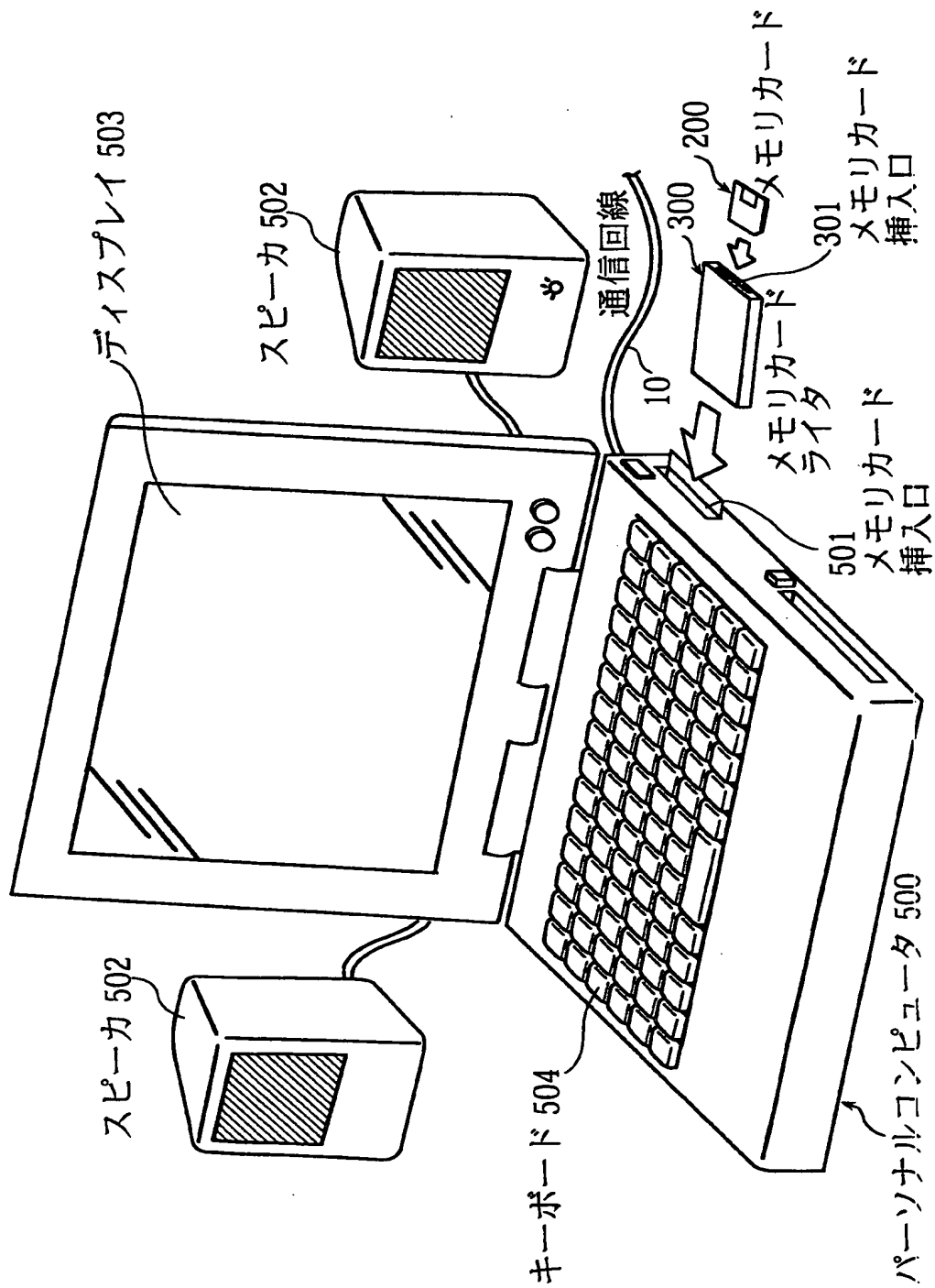
- 4 3 2 暗号部
- 4 3 3 復号部
- 4 3 4 相互認証制御部
- 4 4 0 通信部
- 4 5 0 制御部
- 4 6 0 復号部
- 4 7 0 著作物記憶部
- 4 8 0 再生部
- 4 9 0 操作部

【書類名】 図面

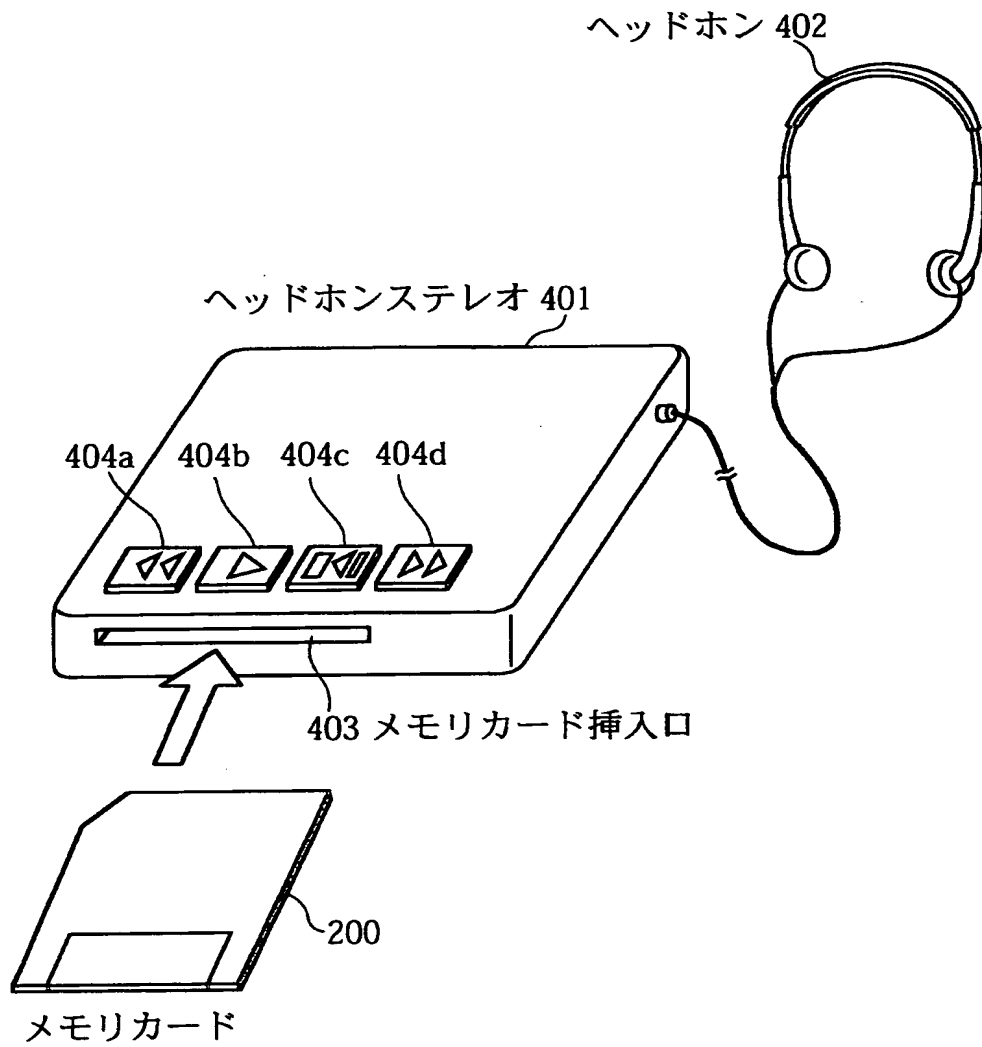
【図 1】



【図 2】

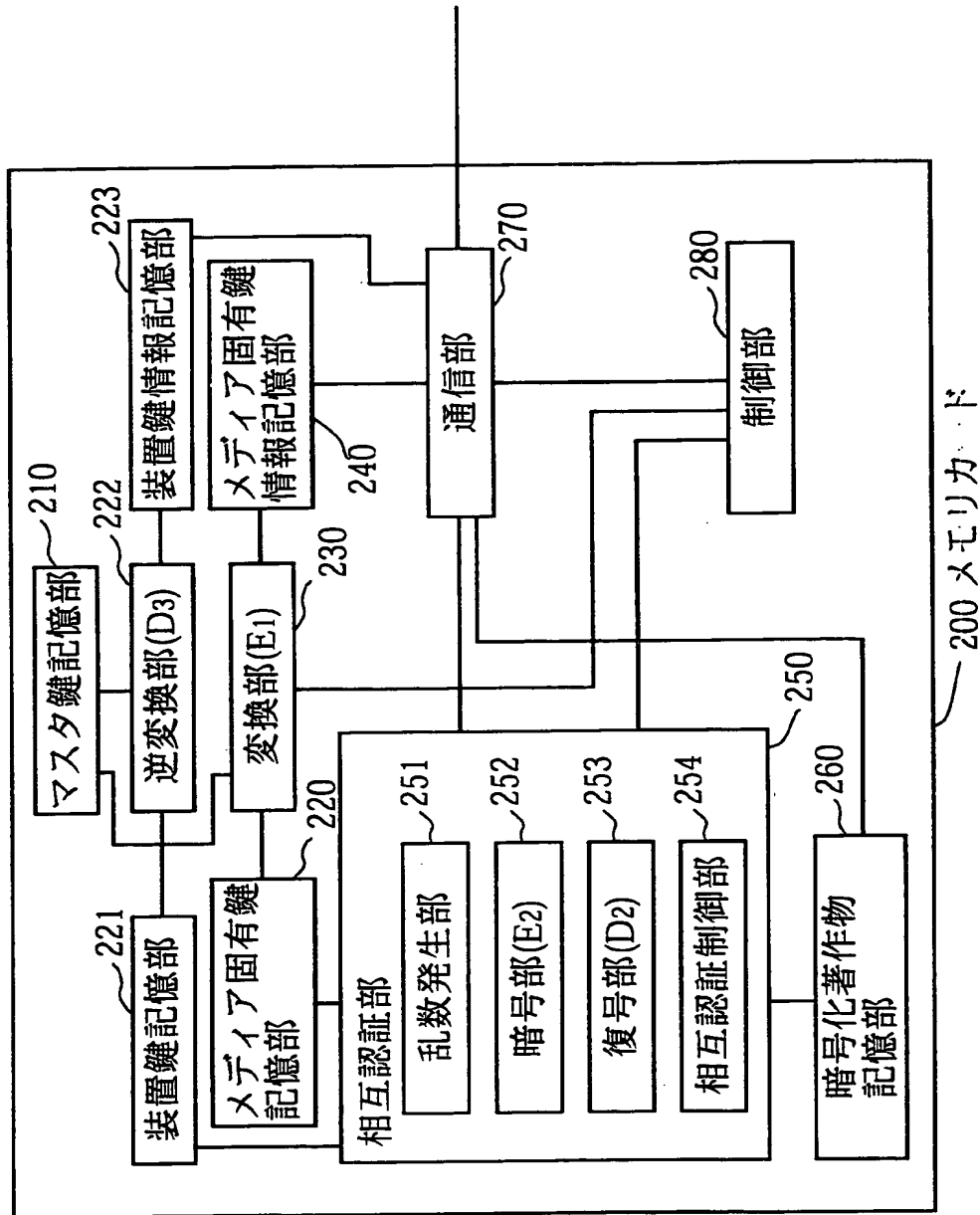


【図 3】

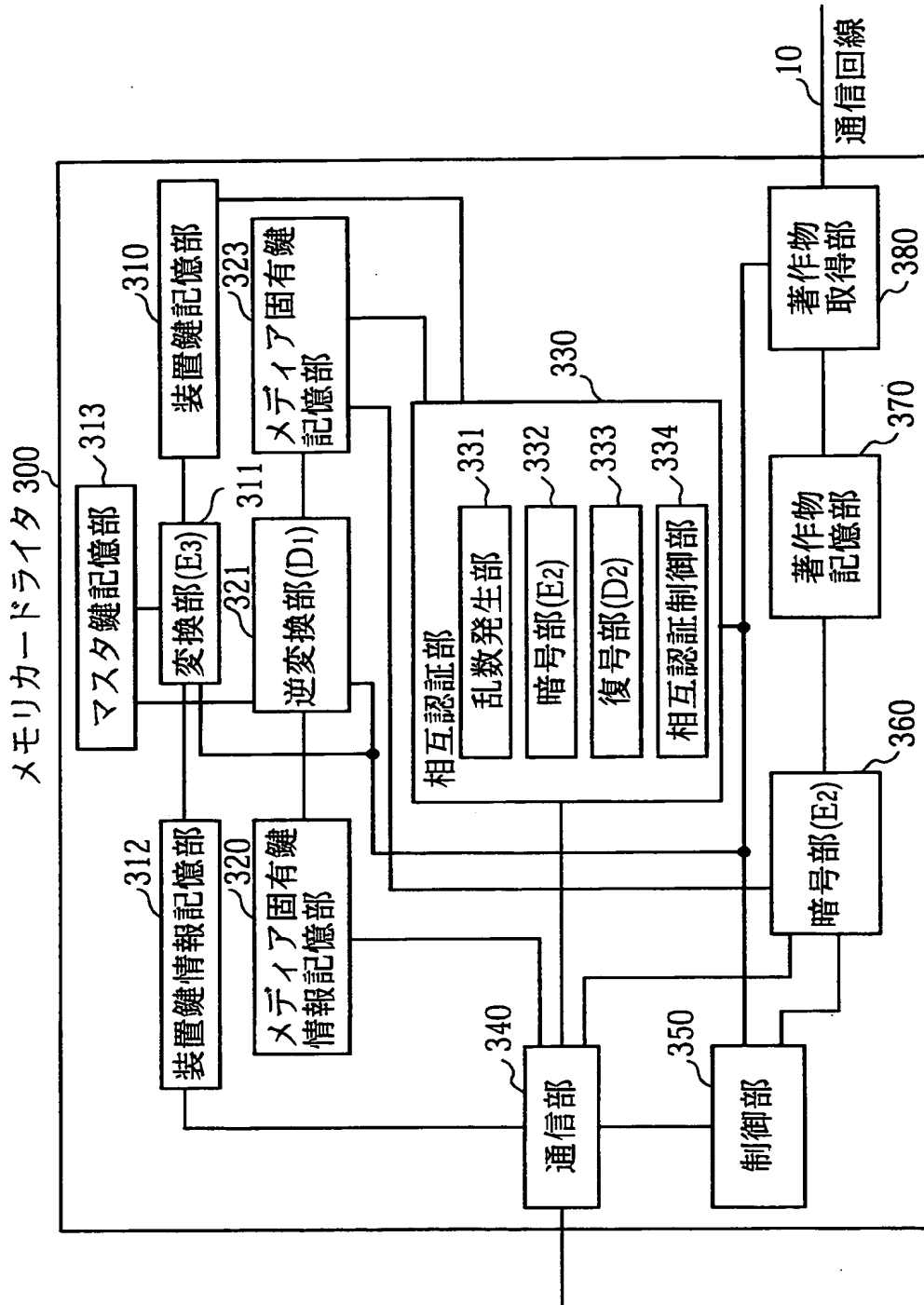




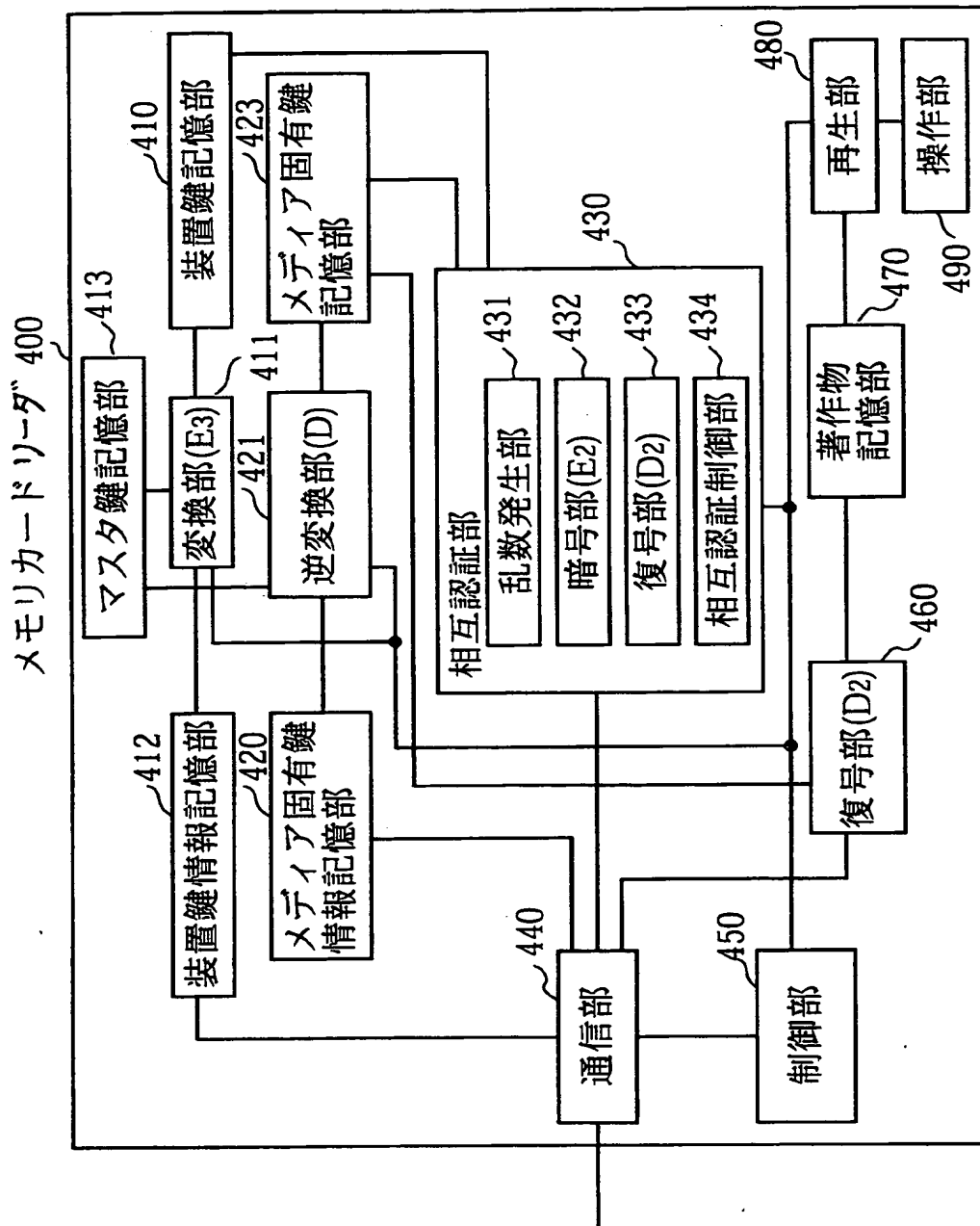
【図 4】



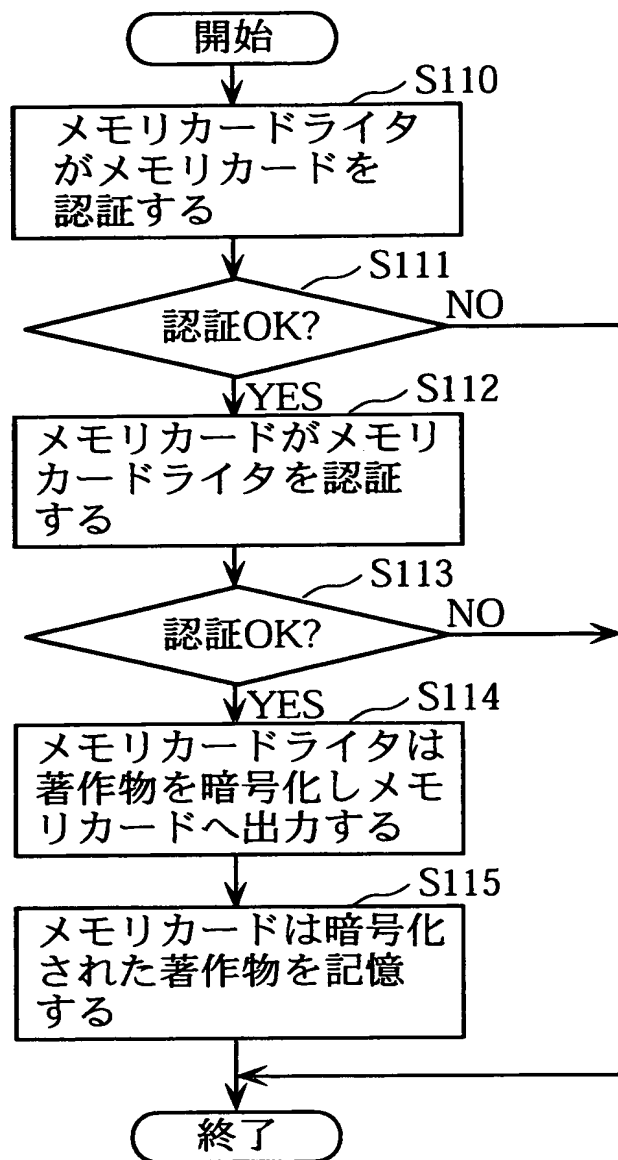
【図 5】



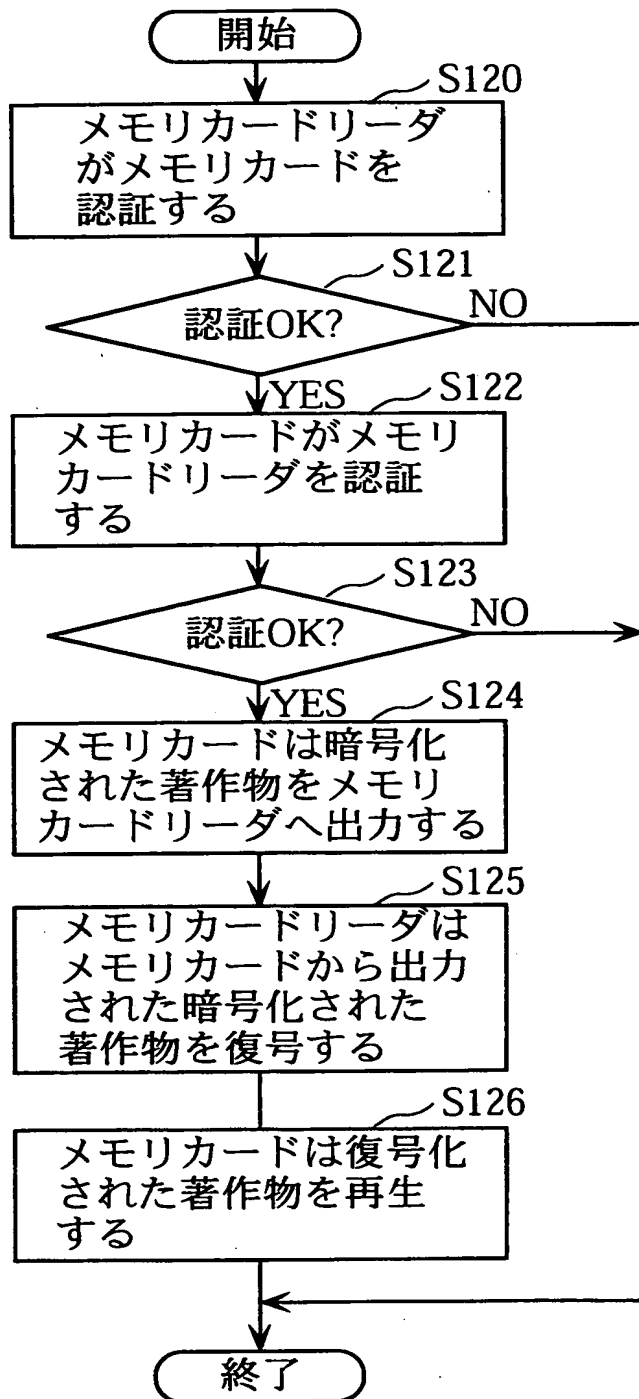
【図6】



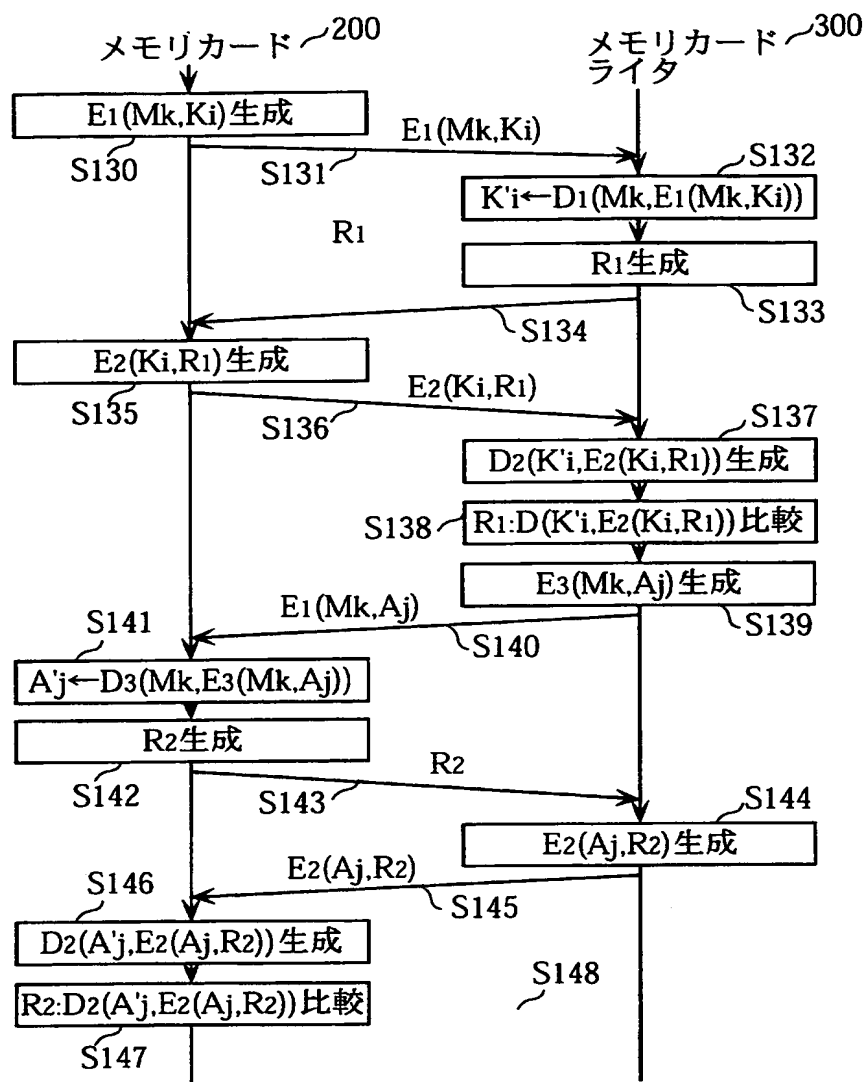
【図 7】



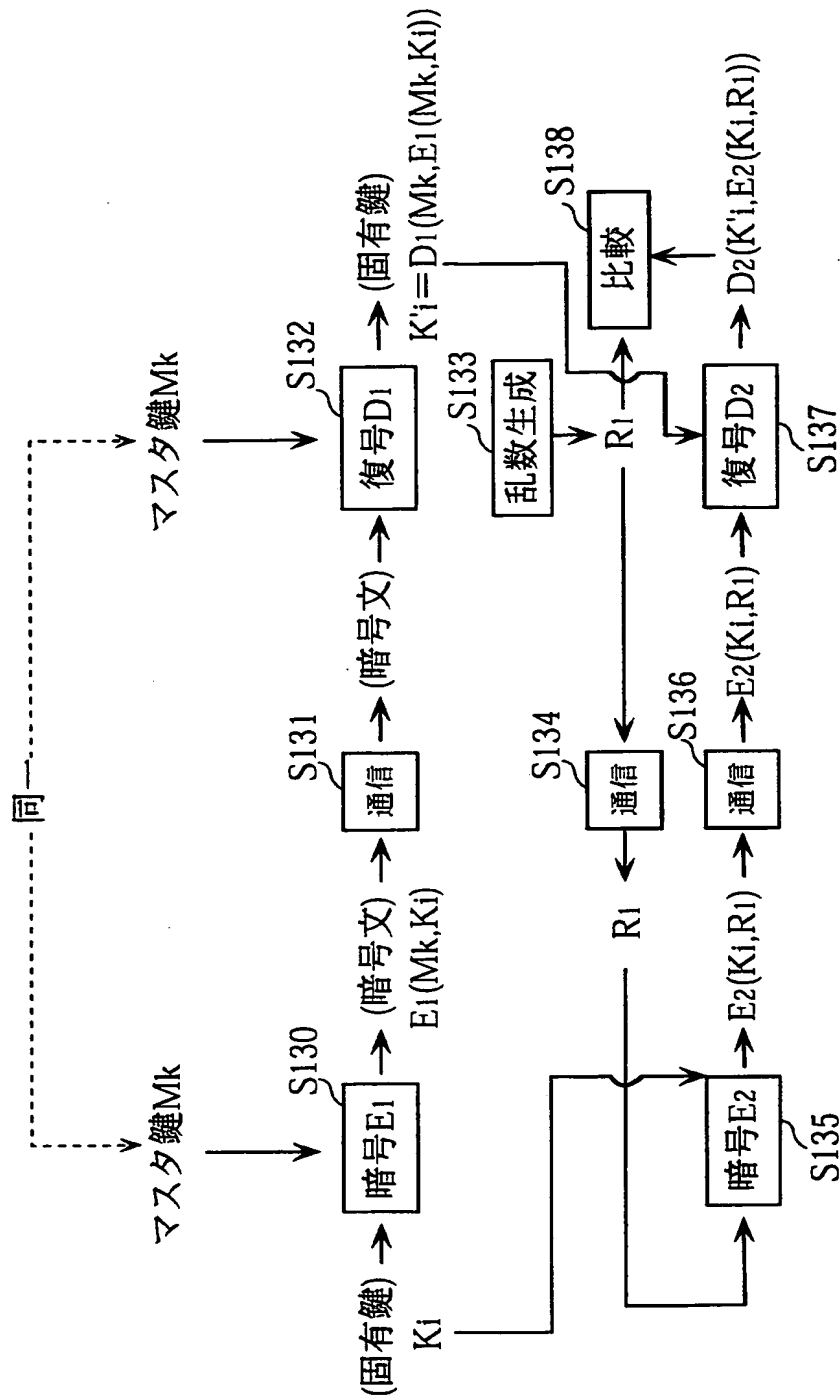
【図 8】



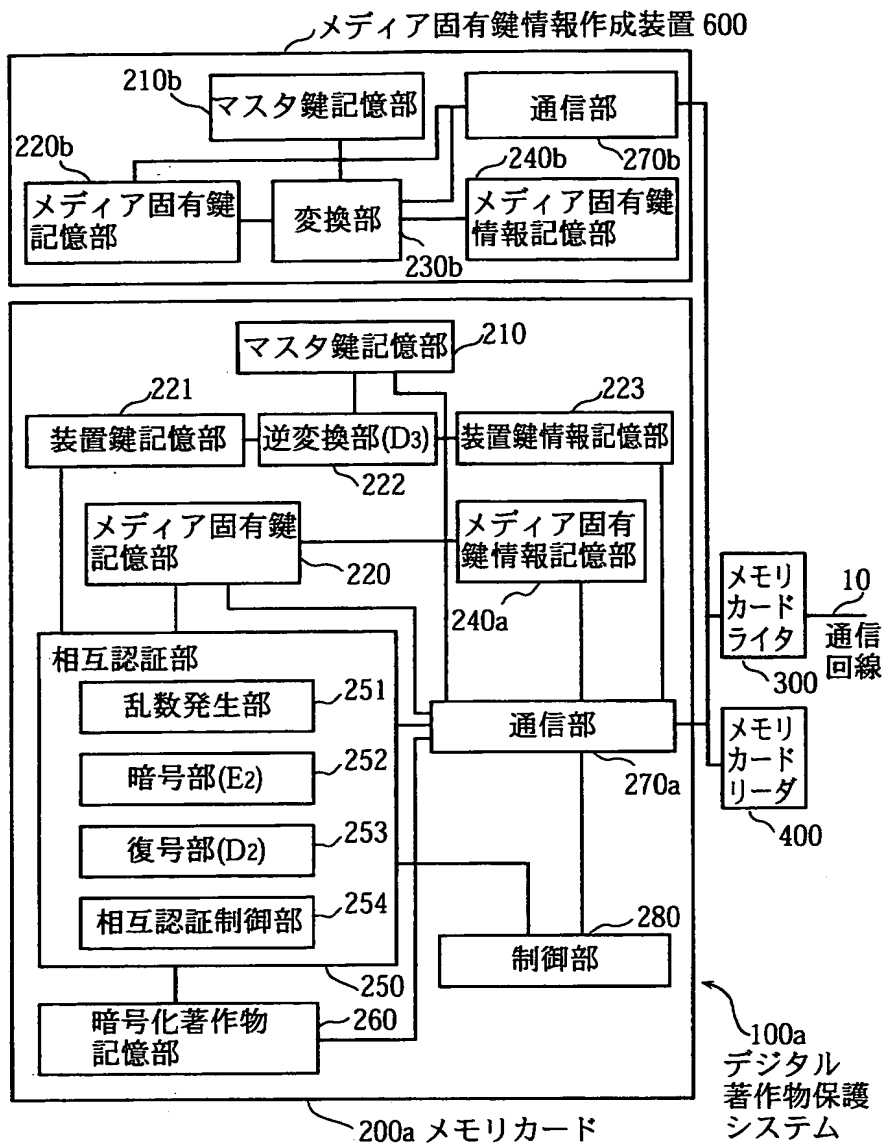
【図 9】



【図 10】

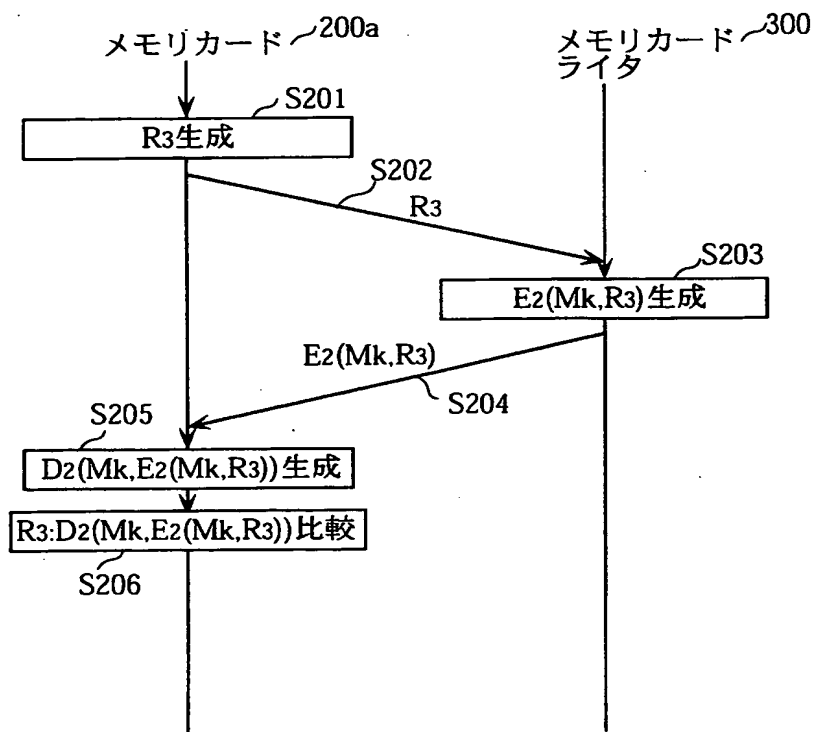


【図 11】

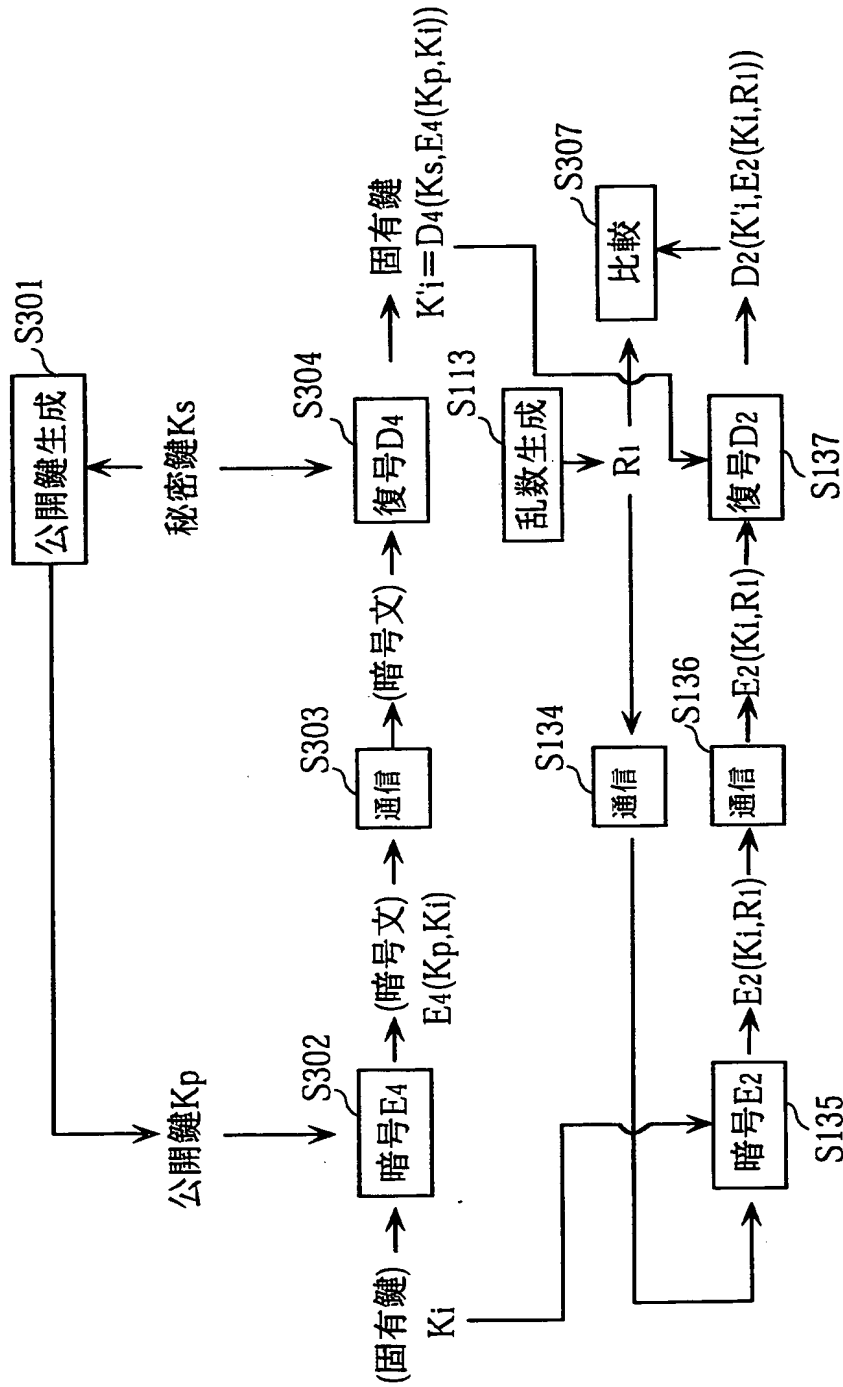




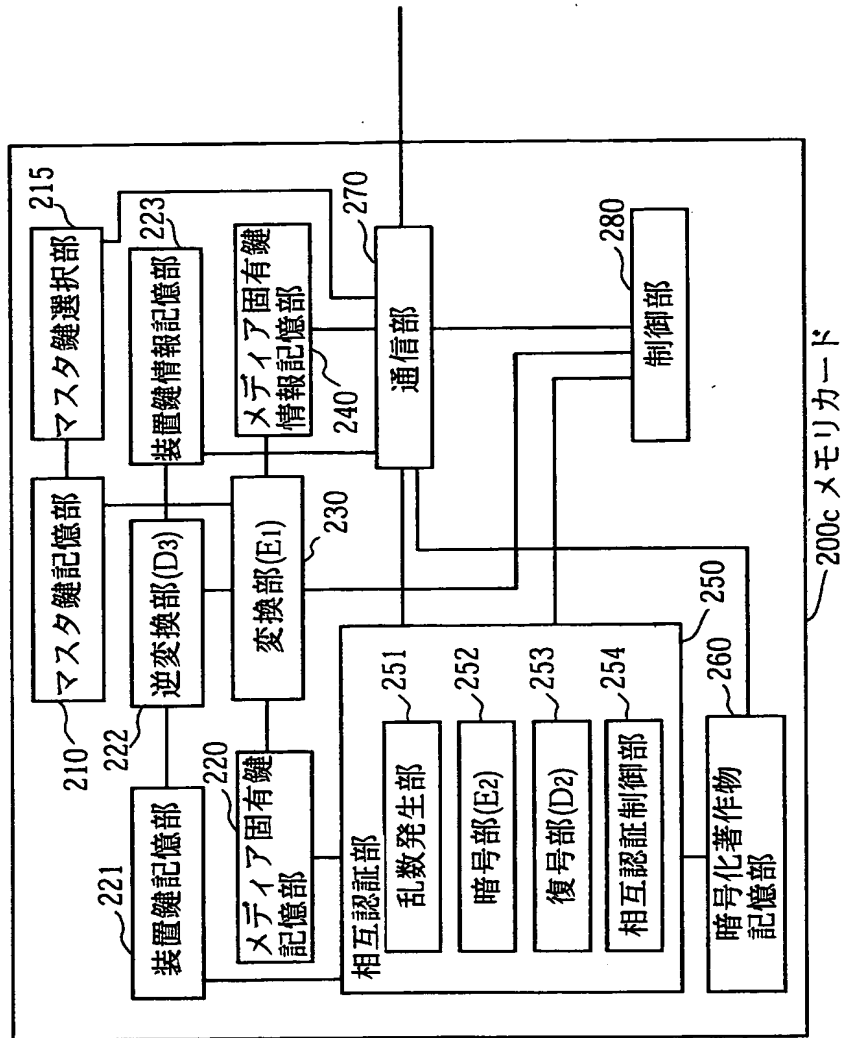
【図 12】



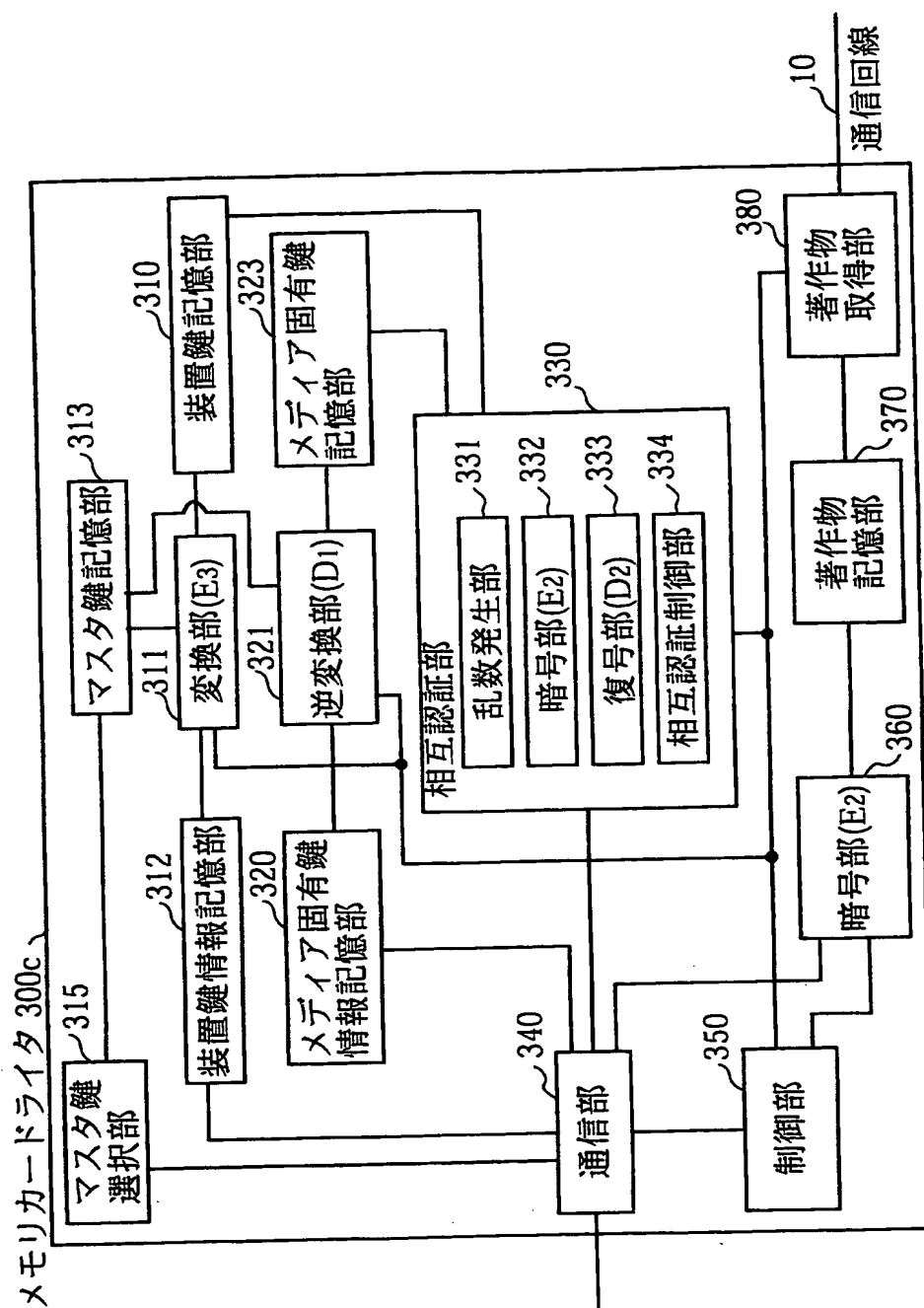
【図 13】



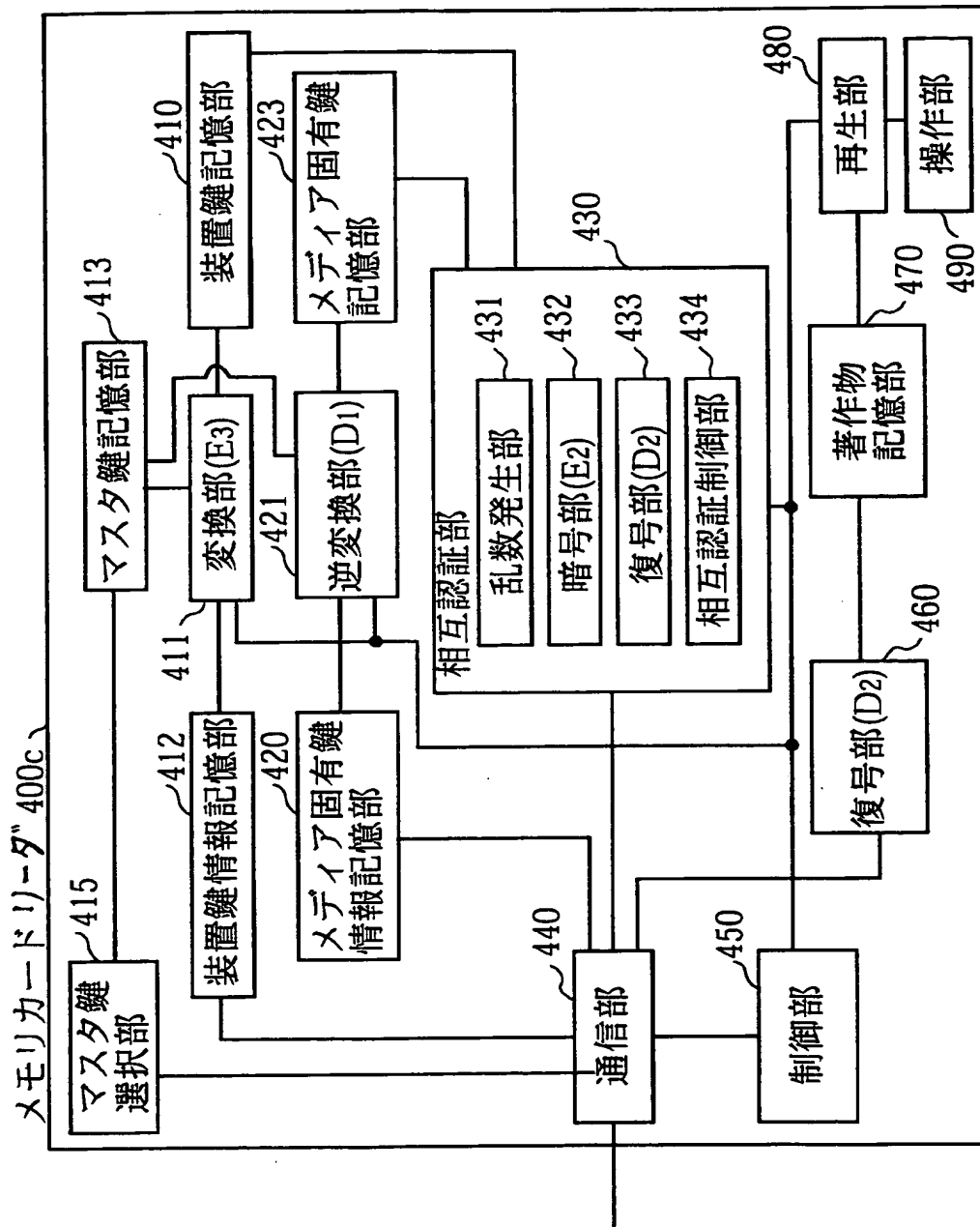
【図 14】



【図 15】



【図 16】



【書類名】 要約書

【要約】

【課題】 外部から取り出したデジタル著作物を不正に記録媒体へ書き込むことと記録媒体に記録されたデジタル著作物を不正に再生することを防止する。

【解決手段】

メディア固有鍵記憶部 220 はあらかじめ一つの固有鍵  $K_i$  を記憶し、変換部 230 は読み出した固有鍵  $K_i$  から暗号化固有鍵  $J_i$  を生成し、乱数発生部 251 は乱数  $R_2$  を生成し、暗号部 252 は乱数  $R_1$  から暗号化乱数  $S_1$  を生成し、復号部 253 は暗号化乱数  $S_2$  から乱数  $R'_2$  を生成し、相互認証制御部 254 は乱数  $R'_2$  と乱数  $R_2$  とを比較し一致すればメモリカード 200 が装着されたメモリカードライタ、メモリカードリーダーが正しい装置と認証する。

【選択図】 図 4

【書類名】 職権訂正データ  
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000005821

【住所又は居所】 大阪府門真市大字門真 1006 番地

【氏名又は名称】 松下電器産業株式会社

【代理人】 申請人

【識別番号】 100090446

【住所又は居所】 大阪市北区豊崎 3 丁目 2 番 1 号 淀川 5 番館 6 F  
中島国際特許事務所

【氏名又は名称】 中島 司朗

【代理人】

【識別番号】 100109210

【住所又は居所】 大阪市北区豊崎 3 丁目 2 番 1 号 淀川 5 番館 6 F  
中島国際特許事務所

【氏名又は名称】 新居 広守

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社